Data and Results Team Data Privacy Policy

January 2024

About

This document provides an overview of Promise Partnership's data privacy policies, including a data disclaimer, data retention policies, breach and disclosure policies, and data security policies.

As an organization, we take data privacy and security seriously and have set up multiple controls to make sure we and our partners are good stewards of data. Promise Partnership Utah has worked with legal teams, Granite School District, and Utah State Board of Education to set up strict privacy and data sharing protocols, including the development of a student data consent form that, if signed by parents, allows the sharing of student academic data with Promise Partners to provide better, more comprehensive supports for students.

Statement of Compliance

At Promise Partnership Utah, we understand the importance of robust protections for data privacy and security. We comply with federal and state law regarding data privacy and sharing. Within our partnership with Granite School District, we have developed and agreed to multiple controls to ensure we and our partners are good stewards of both student-level and non-identifiable aggregate data. Our organization has a commitment to the protection of student data and implements policy to ensure compliance with state and federal law.

Promise Partnership Utah is committed to protecting the privacy of student education records in accordance with the Family Educational Rights and Privacy Act (FERPA). As a nonprofit organization, we adhere to FERPA regulations by safeguarding the confidentiality of student records and ensuring that access to these records is limited to authorized personnel only. Any disclosure of student information is done in compliance with FERPA guidelines and with the consent of the student or their parent/legal guardian, as applicable. Our organization maintains strict policies and procedures to ensure FERPA compliance, including training staff on the proper handling and protection of student records. For questions or concerns regarding FERPA compliance, please contact Nicole Davis at nicole.davis@promisepartnership.org.

Policies

Data privacy and protection policies drafted by Promise Partnership Utah's Data and Results Team.

Disclaimer Statement

The disclaimer statement included below should accompany any data deliverable provided by Promise Partnership Utah to partners. The contact space at end should be replaced with the data specialist who prepares and delivers the data. Otherwise, the contact will be Nicole Davis at nicole.davis@promisepartnership.org. If the data deliverable includes student-level data where PII or an n-size less than 11 will be disclosed, add the "Student-Level Data Disclaimer Add-On" paragraph to the end of the general disclaimer in your deliverable.

General Disclaimer

"The data provided by Promise Partnership Utah are subject to the following:

> **Data Sources:** Data are collected under data-sharing agreements, potentially excluding the complete student population.
> **Analytical Processes:** Analytical methods may differ from federal, state, or district-level reporting.
> **Entity Responsibility:** This data does not represent official reporting by other entities.

Although the information found in this report has been produced and processed from sources believed to be reliable, no warranty, express or implied, is made regarding accuracy, adequacy, completeness, legality, reliability, or usefulness of any information. This disclaimer applies to both isolated and aggregate uses of information. The information contained herein is provided on an "as is" basis. Data users are also cautioned to consider the provisional nature of the data before using it for decision making. The user assumes the entire risk related to use of the data.

For inquiries, contact [NAME] at [EMAIL]."

Student-Level Data Disclaimer Add-On

"This data deliverable includes student-level where Personally Identifiable Information is disclosed, or the n-size for a particular group is less than 11 students. Pursuant to the signed Data Sharing Agreement between our organizations,

(1) All individuals viewing this data must have a signed Data Confidentiality Agreement on file with Promise Partnership Utah.
    a. *If you would like to check if an individual has a signed DCA, please reach out to Nicole Davis at nicole.davis@promisepartnership.org.*
(2) The portions of this deliverable that contain PII, or data for groups of students that are smaller than 11 individuals, are not to be shared externally under any circumstances for risk of disclosing PII, and the potential re-identification of students.

Please refer to your signed Data Confidentiality Agreement for more information on your data privacy commitment as a Promise Partner."

Data Retention Policies

If the Educational Records are provided in order to conduct a study, audit, or evaluation of an educational agency or institution, Promise Partnership will destroy the Educational Records when no longer necessary for the specific purpose for which the information was provided. This requirement will not apply to Educational Records obtained with the Student's written consent.

Upon written request from Granite School District, Promise Partnership Utah shall dispose of or provide a mechanism for Granite School District to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

Upon termination of this DSA, if no written request from Granite School District is received, Promise Partnership Utah shall dispose of all Student Data after providing Granite School District with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account. Granite School District may employ a "Directive for Disposition of Data" form. If Granite School District

and/or Promise Partnership Utah employ a “Directive for Disposition of Data”, no further written request or notice is required on the part of either party prior to the disposition of Student Data.

The Parties will not destroy any Educational Records subject to an outstanding request for inspection or review.

N Size for Suppression

In most cases, PPU follows the Utah state data standard of masking or suppress any population with N size < 11. For n size < 11, Promise Partnership Utah will generally suppress the data entirely and show “data not available” rather than risk exposure of student-level data through a too-small population size.

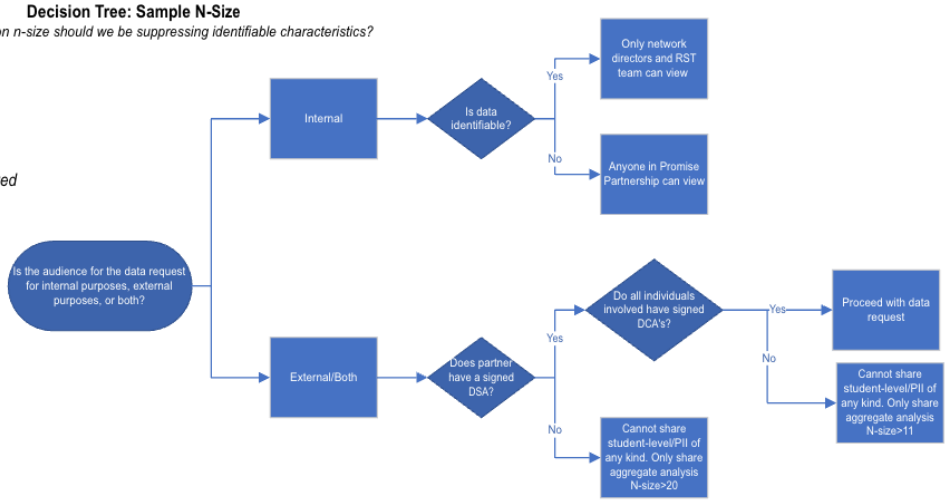
In some cases, the populations that Promise Partnership Utah works with are far fewer than standard populations Utah state is working with that dictate the threshold of n size = 11. In those cases, Promise Partnership Utah will suppress or mask data with an n size < 20, and the analyst may choose to display results within a +/- 10% range.

In rare cases where a partner requesting use of GSD data does not have a data sharing agreement in place with Promise Partnership Utah, we check with GSD on a case-by-case basis to confirm whether masking/suppressing at an n size <20 is sufficient.

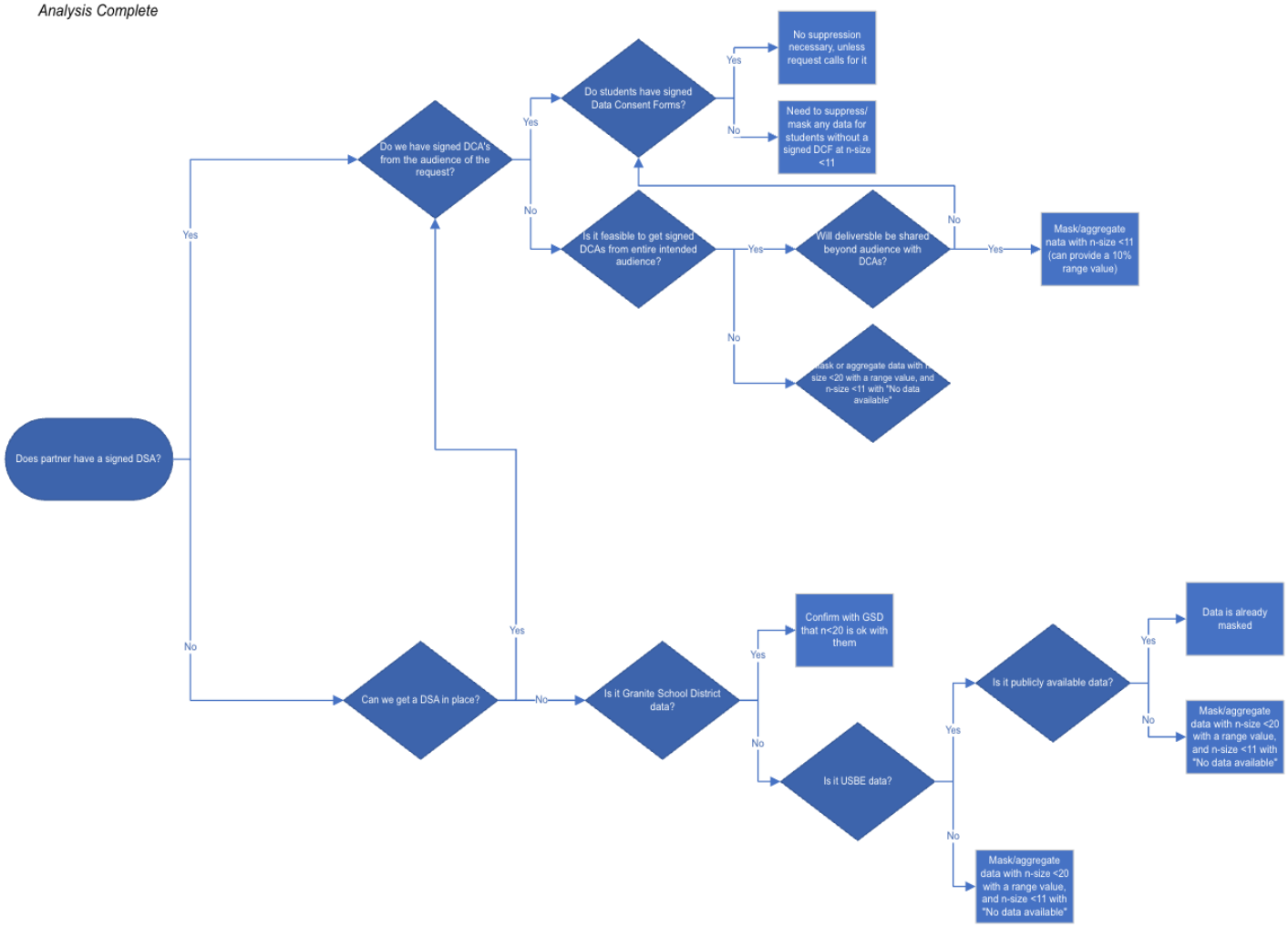
Decision Tree: Sample N-Size

At what population n-size should we be suppressing identifiable characteristics?

Request Recieved



Analysis Complete



Data Quality Disclaimer

This disclaimer can be used to accompany data deliverables to external partners. Specifically, where the reported data may be compared to state or district values, this data quality disclaimer can help account for differences in sourcing, analysis, and interpretation from publicly available sources.

> *"While every effort has been made to ensure the accuracy of the data provided, we cannot guarantee that it will match publicly available data from other entities due to variations in data sourcing methods, timing, and interpretation. Users are encouraged to cross-reference information from multiple sources for comprehensive analysis and decision-making."*

Comparing outcomes from different schools

This disclaimer should accompany data deliverables that report outcomes on a school or district level. Stating that our data should not be used to draw conclusions about groups of students is critical to ensuring its correct interpretation.

> *"Though the data here are believed to be prepared well, schools of varying sizes, funding, or demographic distributions may not be comparable to other reporting. This data should never be used to draw conclusions about a school or district in its entirety."*

Breach and Disclosure Policy

In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by Promise Partnership Utah or a Promise Partner, Promise Partnership Utah shall provide notification, in writing, to the data-owning institution within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Promise Partnership Utah shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by Promise Partnership Utah and as it becomes available:

a. The name and contact information of the reporting LEA subject to this section.

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

c. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

d. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Promise Partnership Utah agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Promise Partnership Utah further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide data-owning institutions, upon request, with a summary of said written incident response plan.

(4) Data-owning institution shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from a Partner's use of the Service, Promise Partnership Utah shall cooperate with Partner to the extent necessary to expeditiously secure Student Data.

There are varying degrees of risk associated with the types of data handled by Promise Partnership Utah. PII is the highest level of risk, de-identified data has a lower level of risk, and anonymized data is the lowest level of risk.

Incident Response Plan

Detection and Reporting

Any employee who suspects or detects a data breach must report it to the Senior Director of Technology and the IT Support Technician within 24 hours of detection. Reports must include details such as the nature of the breach, the type of data affected, the owner of the data, and any known or suspected causes.

Assessment and Investigation

The IT Security team will work with the Data and Results team to promptly assess the reported breach to determine its scope, severity, and potential impact. An investigation will be conducted to identify the root cause of the breach and assess any vulnerabilities in systems or procedures that contributed to the incident.

Containment and Mitigation

Immediate steps will be taken to contain the breach and prevent further unauthorized access or disclosure of sensitive data. Mitigation measures will be implemented to minimize the impact of the breach on affected individuals and the organization.

Notification

If the breach involves the unauthorized disclosure of sensitive data, affected individuals will be notified by the Data Specialist whose role includes student data privacy, with help from the IT Security team, in accordance with applicable laws and regulations.

Regulatory authorities and other relevant stakeholders will also be notified as required by law.

Response Coordination
A cross-functional response team will be convened to manage the organization's response to the breach, including legal, IT, communications, and executive representatives. The response team will coordinate efforts to address the breach, communicate with affected parties, and implement corrective actions to prevent future incidents.

Documentation and Reporting
All aspects of the breach, including detection, response, and remediation efforts, will be thoroughly documented. A post-incident report will be prepared by the IT Security team and Data and Results team to analyze the causes of the breach, evaluate the effectiveness of the response, and recommend improvements to prevent similar incidents in the future.

Training and Awareness
Regular training and awareness programs will be conducted to educate employees about their responsibilities in preventing and responding to data breaches. Employees will be informed of their role in reporting suspicious activities and maintaining the security of sensitive data as part of the annual FERPA training.

Non-Compliance
Failure to comply with this incident response plan may result in disciplinary action, up to and including termination of employment or contract, and may expose individuals to legal liabilities.

Review and Revision
This policy will be reviewed annually and updated as necessary to reflect changes in technology, regulations, or business practices.

Student Level Data and Aggregate Data Analysis

Per our Data Sharing Agreement (DSA) with Granite School District, there are a limited number of PPU staff that can see student-level data. In the DSA, these individuals are listed according to role.

The Promise Partnership staff with access to student-level GSD data include:

- Senior Director of Technology who is the only team member with direct access to the data warehouse.
- Data Specialists who analyze student-level data and create non-identifiable reports for internal and external partnership members.
- Promise Partnership Network Directors who can view individual and aggregate-level data to inform strategies.
- Where students have signed data consent forms, this data can also be shared with Partners that work directly with students (such as in afterschool programs).

- In other cases, deidentified aggregate level data can be shared to other internal and external partnership members.

Access to student-level data is dependent on senior management's authorization and the individual's position in the organization and work assignment. Access rights are associated with the individual's roles and responsibilities and the information resources necessary to do their work. Individual access rights are reviewed on an as-needed basis, which includes termination of employment and change in function and/or role. Access is not granted until a Promise Partnership individual has read and signed the internal data privacy policy and completed the appropriate policy review and training.

Each individual at a relevant Promise Partner organization signs a data confidentiality agreement, personally committing to specific practices and mindsets around data use and security. Individual-student level data may only be shared with other Promise Partners working together to support student and school goals when there is a data consent form on file for the student.

Deidentified aggregate level data can be shared to other internal and external partnership members, presuming there is a strong use case, and the entire partnership agrees to the stance toward data outlined in the Promise Partnership Data Agreement.

The data shared with Promise Partnership Utah from Granite School District is used to measure the impact of interventions on student outcomes. We also use GSD data to fill data requests from priority partners including Salt Lake County Youth Services (SLCoYS), Promise South Salt Lake (PSSL), Asian Association of Utah (AAU), Utah Afterschool Network (UAN), Millcreek Promise, and others. The data provided is always de-identified aggregate analysis unless student-level data is specifically requested, and only regarding students for whom a signed Data Consent Form is recorded in the Granite District Data Warehouse. Any time we share student-level data with a partner, we document the request, data used, and any associated deliverables.

There are very few use cases that require student-level data within our organization or among our external/partner data requests. In rare cases where student-level data is essential to a request, we follow masking protocols. Masking protocols include creating a pseudo identification number for students, schools, and/or programs participated in rather than divulging true student, school, or program names and ID numbers. De-identification also includes the removal of any PII, including but not limited to:

- Names,
- Student IDs,
- Addresses,
- Phone Numbers,
- Birthdates

We may also suppress information such as race/ethnicity, gender, school, or more in cases of a small sample size. This practice protects students that may belong to a smaller demographic group from identification, even in aggregate data.

Secure Data Transfer Process

Any student-level or personally identifiable information must be shared using a secure data transfer upload. Other forms of data, such as directory information from a school, should also be shared using this process wherever possible.

A secure transfer is not required where the following has been provided by the school to PPU:

(1) A list of variables designated by a school as directory information in their annual notification to families, and
(2) The variable in question is included in this list of variables.

Secure File Transfer Steps

(1) Navigate to the Schools and Partners SharePoint Site

(2) Navigate to the folder for the partner you want to share data with (either receiving or sending) or create a folder for that partner if they do not have one yet.

(3) Create a new folder for the project you are working on

(4) Share that folder only with the partners' email addresses

a. If the partner should be uploading a file here, ensure that they have edit access. Write a message explaining that this is a secure link that can be accessed only with their email and that they should upload documents here
b. If you are sharing data with the partner, write a message explaining your purpose and upload the file to the folder. (You may want to upload the file before sharing).

(5) Access to this folder will not expire, so do not add unrelated documents here or anything that you do not want to share with the partner

FERPA Compliance

In order to remain compliant with current FERPA regulations, we have implemented the following process to ensure any student we report PII on is protected.

Note: As stated above, the only student-level data PPU has access to is through our Data Sharing Agreement with Granite School District, which is why this process explicitly names them.

Data Consent Form Process