UTAH'S PROMISE DATA CONFIDENTIALITY AGREEMENT

"Data" refers to any Data shared by UP with the Partner, or Data shared by the Partner with UP. Any staff member, consultant, volunteer, or individual who participates in a meeting, email exchange, document review, or other communication where Data related to Utah's Promise Constituents is displayed or discussed (verbally or in writing) are asked to review and sign this Data Confidentiality Agreement, provided that those individuals are not members of the institution that provided the data.

What is Data?

1. **Data is more than numbers.** At Utah's Promise, we think of Data as information to make shifts in policies, practices, resources, and power structures that produce equitable outcomes across a variety of constituent groups. Historically, when people have used the word Data, they've often been talking about Data that is about individuals impacted by our current systems. When we say Data, we also mean Data about outcomes at a community wide scale, Data about systems and institutions, and Data that represents the perspectives and experiences of youth, their family members, and other community members.

I understand I will have access to the scope of Data as described above and to treat it responsibly.

2. **Data is for learning and collaborative improvement.** The Data that we see during our work with UP is for continuous improvement around shared community goals. The purpose of the Data is to track progress and outcomes and to design, test, and improve interventions aimed at moving these outcomes at a population level, especially for those groups most negatively impacted by our current systems. The Data is a reflection on the entire community – we're all responsible for our current reality and future results.

I will use Data for continuous improvement around shared community goals. I will not use Data to indicate the success or failure of one program, organization, school, sector, or minoritized population.

When it comes to Data, what are my responsibilities?

3. **Data should not be re-shared.** Data about specific individuals or about very small groups of individuals can never be shared without prior express permission of the agency providing the Data. Data compiled and presented by an institution about its own programs, initiatives, etc. may be used according to the policies and practices of that institution without restriction.
4. **People come first.** UP will inform clients, students, parents, and other UP constituents whose stories are represented in the Data we use how their information is used generally – for example, by sharing information like what's at: https://promisepartnership.org/data/. Individuals who share their expertise via community research projects coordinated by UP will be informed of how their Data will be used and provide written consent, prior to providing Data. UP will involve those most impacted in the processes of interpreting the Data. This agreement and the conversations UP wishes it sparks is another practice developed to maintain this trust.
5. **Need for ongoing training.** From time to time, Partner may be required to participate in reasonable training on data privacy and security (for example, annual FERPA training).

I will not share Data outside of UP or my organization without the written permission of the Partner that provided the Data and without acknowledgement of the shared accountability for our current realities and for the results that UP commits to holding. I will not share Data with media, funders, or

the general public without written permission of the agency that provided the Data. I will complete reasonable training in Data use as requested by UP.

How should I protect Data?

6. **Data Protection Protocols.** As an individual with access to Data, you agree:

How the Data is intended to be used:

a. UP constituents (students, community members, etc.) and the entities that collect and/or store Data have the right to expect that Data will only be used to support efforts that reflect the intended use under which permission to share the Data with UP was originally granted.
b. No attempt will be made to re-identify any non-personally identifiable information (non-PII) Data to associate it with a Constituent's identity.

I will only use Data for the purpose for which the Constituent granted permission and will not attempt to identify any Constituent using non-PII Data.

How to safeguard physical and electronic Data:

c. Any PII retained electronically or in a hard copy format must be kept secure in accordance with all relevant Data Protection Laws. Accordingly, UP and Partner:
    i. Will refrain from discussing Constituents in public areas
    ii. Will not leave Data in printers, on desktop surfaces, or in public areas
    iii. Will shred (or place in a secure shred bin) Data that is no longer needed, in accordance with all relevant State and Federal student data privacy laws and Data Protection Laws.
    iv. Will store electronic Data using encrypted storage with limited access
    v. Will only share PII through secure methods such as secure links, encryption, and authentication, including multi-factor authentication where available.
    vi. Will use discretion when discussing Constituents over email, particularly if Partner does not have a policy to mitigate mobile risk (e.g., the use of personal handheld devices and tablets as an access point for agency information).

I will use the protocols listed above to safeguard physical and electronic PII Data.

Who should and should not have access to Data:

d. Non-Personally Identifiable Information ("non-PII Data") that is downloaded or printed will be stored in locations that can only be accessed by organizational staff with a legitimate need to have access to such information.
e. Any staff member, consultant, or volunteer of Partner who participates in a meeting, email exchange, document review, or other communication where Data is displayed or discussed (verbally or in writing) must have signed a copy of this Data Confidentiality Agreement, before Data is displayed or discussed. Partner will only share Data with those staff members, consultants, or volunteers of Partner with a legitimate interest in the information and are working with Data according to the Purpose agreed upon in the Data Sharing Agreement. Even if UP does not distribute this Data Confidentiality Agreement at a convening where Data is discussed, UP does not waive the above requirements for confidentiality.
    i. To avoid the possibility of any individual being identified, any Non-Personally Identifiable Information that is shared with an individual not covered by a Data Confidentiality Agreement must include at least eleven individuals.

f. Personally Identifiable Information may not be shared with non-Partners. PII will only be disclosed to Partners who have a legitimate interest in the information and are working with Data according to the Purpose agreed upon in the Data Sharing Agreement.
g. Non-Personally Identifiable Information originated by any other Partners may only be shared with non-Partners when the purpose of sharing includes:
    i. To secure funding from potential funders and to ensure compliance with funding agreements; or
    ii. With a legitimate interest in the information and are working with Data according to the Purpose agreed upon in the Data Sharing Agreement; and
    iii. After receiving written permission from Partner(s) who originated the Data. Written permission from Partner(s) must be granted by an originating Partner with approved authority. Once approved by the originating Partner(s), Data shared with non-Partners must be cited in a format approved by the originating Partner(s) and UP.

I will only share PII Data with Partners with a signed Data Confidentiality Agreement and who are working with Data according to the purpose of the Data Sharing Agreement. I will only share non-PII Data with non-Partners to fulfill the purposes listed above.

What Data you're agreeing to safeguard:

h. These Data Protection Protocols apply only to the Data created or shared as part of the applicable Data Sharing Agreement (a) with UP by the Partner, or (b) by the Partner with UP, and not to any other Data owned by the Partner organization.

I will use these protocols to safeguard Data created by either UP or my organization for the purposes of the Data Sharing Agreement with UP.

7. **Data Breach Notification.** I will notify UP at data.breach@utahspromise.org if I become aware of any actual or potential unauthorized Data disclosure, within 48 hours of becoming aware. UP will respond as outlined in the IT & Data Security Policy located at https://uw.org/financials-and-policies/.

I will notify UP within 48 hours of any potential or actual unauthorized Data disclosure.

I understand that disclosing – verbally or in writing – Data that is shared with me through my organization's partnership with UP could result in dismissal from the relevant programs and/or a termination of funding and other support provided by UP and/or legal action.

By signing, I agree to the full terms and conditions of this agreement.

Name:

Organization:

Title:

Date: