

Tribal Data Policy

Purpose

First Things First (FTF) recognizes the right of tribes in Arizona to regulate research and data collection on their tribal lands. To this end, FTF is committed to obtaining all appropriate tribal approvals for data collection, use, analysis, publication, and sharing. FTF created this Tribal Data Policy to set forth the principles and basic process by which FTF and its collaborators will seek agreements and other approvals with tribes for the collection, use, analysis, publication, and sharing of data related to the provision of programs for children 5 and younger and their families who are living on tribal lands and data related to early childhood professionals working on tribal lands.

This Tribal Data Policy supplements FTF’s Data Security Policy and FTF’s Collaborator Data Policy by providing additional protections for “tribally protected data.”

Background

This Policy was informed by FTF’s experience in securing tribal data collection agreements as part of its process to develop regional needs and assets reports and provide programs and services on tribal lands, as well as insight and feedback obtained through formal consultation between FTF and tribes.

The mission and vision of FTF is to lead and partner in the creation of a family-centered, equitable, high-quality early childhood system that supports the development, well-being, health and education of all Arizona’s children, birth to age 5, so they are ready to succeed in school and in life. This work involves coordination and funding for early childhood development and health programs.

FTF’s work in partnering with tribes has led to the implementation of many programs in tribal communities that expand early childhood education opportunities, support parents in their role as their child’s first teachers, and expand the use of preventive health services and screenings. For example, these include the Quality First program, which supports child care providers in increasing the quality of their programs, Quality First scholarships to make attending a Quality First provider affordable for families of young children, developmental and sensory screenings, early childhood mental health consultation, family, friend, and neighbor care, home visitation, language, literacy and culture in tribal communities programs, and transition to Kindergarten programs.

Under state law, FTF must identify and report on the assets available for these programs and the unmet need for these programs throughout each region of the state in order to determine which programs to fund.¹ FTF must also measure the success of its funded programs by their outcomes for children and

¹ A.R.S. §§ 8-1161(A)-(C) & 8-1192(A)(1)

families.² In order to meet these requirements, FTF collects, maintains, and reports data on the needs and assets available for early childhood development and health programs and on the performance of FTF's funded programs in each region of Arizona. Comprehensive, accurate data is crucial to the success of Arizona's partnerships with tribes and ultimately to the creation of an effective early childhood system.

Policy

FTF and its collaborators must only collect, use, analyze, publish, and share tribally protected data (i) with appropriate tribal approvals, which may require participation in cultural education and community orientation classes, and (ii) in accordance with this Tribal Data Policy, FTF's Data Security Policy, and FTF's Collaborator Data Policy, as applicable. FTF and its collaborators will also protect that data in accordance with tribal agreements, tribal law, this Tribal Data Policy, FTF's Data Security Policy, and FTF's Collaborator Data Policy, as applicable.

In this Policy as well as in the Data Security Policy and Collaborator Data Policy, "Collaborator" refers to an FTF grantee (i.e., grant partner), governmental entity, or vendor (i.e., contractor) assisting with an FTF needs and assets report, conducting an FTF-funded program or service, conducting an informal survey, performing a formal study, or collecting data through other approaches on behalf of FTF. In addition, the term "collect" broadly refers to getting data, such as by collecting, obtaining, receiving, gathering, creating, or acquiring the data, including primary, secondary, and tertiary data and the term "publish" refers to disseminating materials in a printed or electronic format for public distribution (e.g., needs and assets reports, impact reports, fact sheets, annual reports).

Data Definitions

Confidential Data. Confidential data is nonpublic data that identifies individuals or is governed by agreements or laws that limit its viewing, analysis, or dissemination. Confidential data may also include confidential business information. Confidential data may be subject to HIPAA, FERPA, tribal law, or other data regulation.

Limited Distribution Data. Limited distribution data is aggregated data created from confidential data of just a few individuals, which creates a risk that the aggregated data will permit the identification of an individual whose data is included. (See Data Suppression for Publications, below.) Limited distribution data may be subject to HIPAA, FERPA, tribal law, or other data regulation.

Public Data or Publicly Available Data. Public data is data that is readily available to the general public, such as data located on websites, in publications, or in other widely used sources, as well as unpublished

² A.R.S. §§ 8-1151(B)(6), 8-1174 & 8-1192(A)(4)

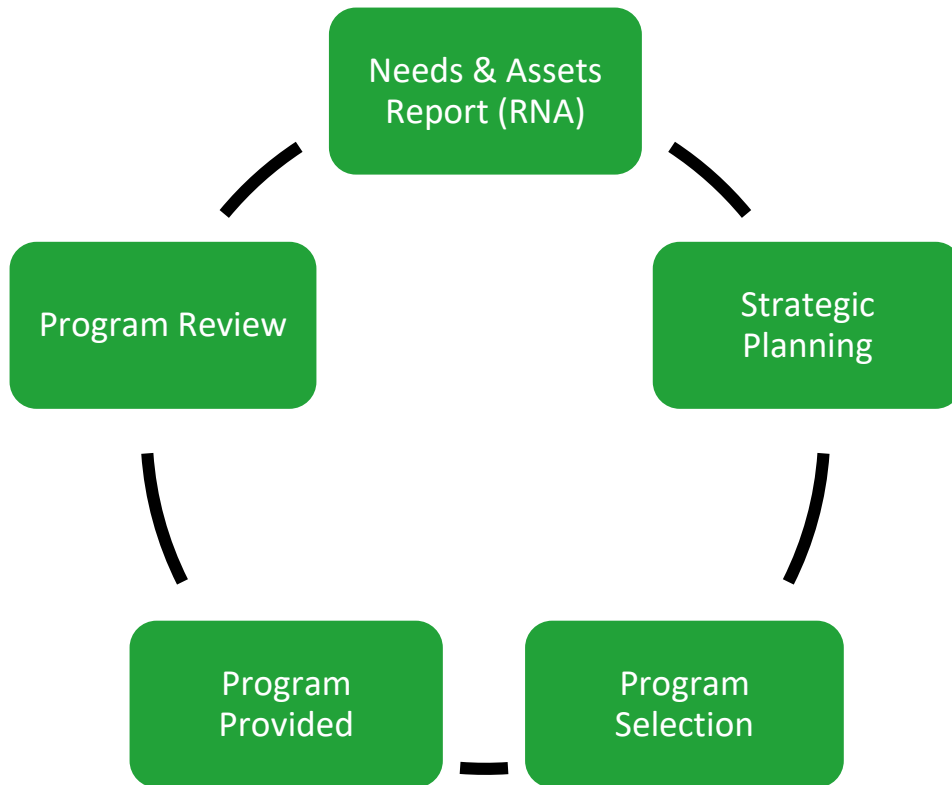
information that members of the public may obtain upon request without needing tribal permission. Public data includes both data published by FTF (e.g., needs and assets reports and impact reports) and data that has been officially released by another organization (e.g., census data). Public data also includes aggregated data, except where the aggregated data constitutes limited distribution data or tribally protected data.

Tribally Protected Data. Tribally protected data is nonpublic data collected from tribal lands of individuals living or working on tribal lands, including nonpublic aggregated data, where the tribe regulates the collection, use, analysis, publication, or sharing of the data. Tribally protected data is considered confidential data except to the extent the tribe has given permission for the data's collection, use, analysis, publication, or sharing, as described in this Tribal Data Policy. Tribally protected data includes nonpublic data FTF collects directly from tribal sources, such as individuals living on tribal lands, tribal programs and departments, tribal Head Starts and child care facilities, and tribally run health care facilities, as well as nonpublic data held outside tribal sources that FTF can only collect with permission from the tribe, such as nonpublic data held by Indian Health Services (IHS) and the Inter Tribal Council of Arizona (ITCA). Tribally protected data does not include publicly available data from any source.

Data Collection–Reasons

FTF collects data and other information from tribal governments and entities, early childhood professionals working on tribal lands, and families living on tribal lands for two primary purposes, which are related to the provision of programs for young children and families living on tribal lands and early childhood professionals working on tribal lands: (i) needs and assets reports and (ii) program and service administration and implementation. Occasionally, FTF may also collect data and other information from people living or working on tribal lands for other purposes using informal surveys, formal studies, or other informal and formal approaches.

FTF often collects data through a collaborator. Sometimes the collaborator is a tribal entity. FTF publishes some of the collected data and information, such as in data reports and other hard copy and online documents, to guide decision-making, measure the progress made in obtaining outcomes for children and families, and increase public awareness of the needs of young children.



Needs and Assets Reports

FTF collects data in order to conduct a statutorily required assessment of each FTF region’s needs and assets every two years. This legal requirement applies to FTF designated geographic regions in which tribal lands are located and FTF regions where a tribe elects to have its tribal lands treated as a separate FTF region. See A.R.S. § 8-1161.A-C.

FTF regional partnership councils use the data in their respective needs and assets reports to develop plans about what programs to fund in their regions. See A.R.S. § 8-1161.D. These FTF-funded programs benefit young children and families living on tribal lands and early childhood professionals working on tribal lands by directly serving them.

Programs and Services

Administration

FTF and its collaborators provide early childhood development and health programs. These collaborators include tribal entities. FTF or its collaborator collects information from individuals who are directly benefiting from a program for the purpose of administering that program. For example, this data might include the recipient’s name, birthdate (e.g., to verify age eligibility), and address (e.g., to provide home visiting services). The collection of this type of information benefits young children and families living on tribal lands and early childhood professionals working on tribal lands because the programs could not be provided without this information.

Implementation

FTF also regularly collects data to assess the effectiveness of its funded programs in meeting program requirements and in achieving their intended outcomes for young children and their families. This type of data (also known as implementation data or program outcome data) benefits young children and families living on tribal lands and early childhood professionals working on tribal lands by helping to ensure that financial resources are focused on programs that make a positive impact on those served.

Implementation data addresses how a collaborator is meeting contractual target service units (e.g., number of caregivers enrolled) and performance measures (e.g., percentage of caregivers completing a family, friend, and neighbor care series compared to total number of caregivers enrolled).

Implementation data begins with the collection of data by the collaborator. This data might include, for example, the number of people served and sociodemographic information (e.g., age, income level, race, and ethnicity) about those served. Implementation data may also occasionally come from program satisfaction questionnaires, exit surveys, interviews, or pre- and post-tests, which are methods used to gauge how effectively a program increased knowledge or skills or otherwise benefitted a family or early childhood professional.

FTF primarily receives implementation data from quarterly and annual reports submitted by its collaborators, including contracted tribal service providers. FTF may also receive implementation data of a collaborator in other ways, such as from a national organization that oversees the program model the collaborator is using (e.g., Parents as Teachers home visitation model) or from another data collection system housing FTF collaborator data, such as the Arizona Early Childhood Workforce Registry.

Informal Surveys and Other Informal Approaches

From time to time, FTF may use informal data collection approaches to gather information to help guide FTF's efforts. Informal approaches can provide quick insights for initial exploration or decision making. The most common informal approach is online surveys, which often do not even collect participants' names or city. Survey results can assist with, for instance, community awareness efforts, early childhood systems change projects, media use, and future program opportunities. For example, FTF has done informal surveys seeking input and feedback on: FTF's strategic planning, people's content preferences for the FTF newsletter, how child care has impacted businesses, and child care challenges for working parents with young children. These informal surveys do not require special skill to create or to review the results. Feedback from these informal surveys helps FTF be a little more aware of and responsive to people and provider's needs.

This section applies to informal surveys and other informal data collection approaches that are not for program implementation or needs and assets assessments purposes. If an informal data collection approach is part of program implementation or a needs and assets assessment, then the earlier sections on program implementation and needs and assets assessments, respectively, apply in that instance instead of this section.

Formal Studies and Other Formal Approaches

Once in a while, FTF may use a formal study or another formal data collection approach to better understand the needs of young children and their families or early childhood professionals or to better understand the effectiveness and benefits of certain programs (e.g., Quality First validation study³) statewide or in specific regions. In most cases, an FTF collaborator carries out these formal approaches on FTF's behalf. Trained researchers design and oversee formal studies and use structured methodologies to support the credibility and rigor of the findings.

Data Collection-Requesting Approval

FTF recognizes that a tribe's approval process to collect tribally protected data may vary depending on the purpose of the data (e.g., needs and assets report or program implementation), the data sources (e.g., primary or secondary) and the sensitivity of the type of data (e.g., number of screenings versus the results of the screenings). FTF will not assume that the approval process completed for one set of data is the same for a different set of data.

For FTF-funded programs, the request for authorization to collect program administration and implementation data should accompany the request to conduct these programs on tribal lands.

Requester:

- If FTF will be performing tribally protected data collection itself, FTF will first ascertain the tribe's process for requesting and accessing the desired data and follow the tribe's specified approval process.
- If an FTF collaborator will be collecting tribally protected data to assist with a needs and assets report, to conduct an informal survey, or to perform a formal study on behalf of FTF, then FTF will take the lead in securing the appropriate tribal approvals for the data collection.
- If an FTF collaborator will be performing tribally protected data collection for an FTF-funded program, then FTF will require the collaborator to obtain all appropriate tribal approvals to collect the data unless FTF notifies the collaborator in writing that FTF has obtained the approvals or that FTF will take responsibility for obtaining the approvals.
- If the FTF collaborator is the tribe itself or a tribal entity, that is if the tribe or a tribal entity has contracted with FTF to provide an FTF-funded program, then the contract will represent tribal approval to collect program administration and implementation data unless the tribe or tribal entity notifies FTF that FTF needs to take additional steps for approval.

³ https://www.firstthingsfirst.org/wp-content/uploads/2018/02/AZ_QF_Phase_1_Report.pdf

Data Collection–Collaborator Use of Data

Where an FTF collaborator will collect tribally protected data, the collaborator will need the appropriate approvals from the tribe to collect and use the data or share the data with any third party other than FTF. This includes obtaining appropriate approvals in situations where the collaborator has an additional funding source (e.g., federal government) to which the collaborator has to report data as well as in situations where the collaborator is an affiliate of an evidence-based program/service model (e.g., Parents as Teachers home visitation model) and has to share certain information with the national organization that oversees the model. The requirements for collaborators are described in more detail in FTF’s Collaborator Data Policy.

Data Collection–Agreements

In many instances, a tribe requires formal approval (e.g., Tribal Resolution, MOU, letter from a tribal official) before FTF and its collaborator may collect, use, analyze, publish, or share tribally protected data. FTF refers to this formal approval as a “data collection agreement,” regardless of form.

FTF will follow the provisions of a data collection agreement with a tribe. In the case of a conflict between a provision in the data collection agreement and this Tribal Data Policy, FTF will follow the provision in the data collection agreement.

When FTF needs a data collection agreement, FTF or its collaborator should provide the tribe with the following information about the requested tribally protected data, as applicable:

- the data to be collected, including the context for and background on the data and target populations.
- the sources of the data, including when possible, the organizations providing the data, the data fields to be collected from each organization and whether the data is disaggregated by race, ethnicity or tribal membership.
- examples of possible data collection methods.
- the allowed uses for the data, including descriptions of the final products the data is to be published in.
- the specific measures in place to ensure data security and the confidentiality of individuals whose data is collected.
- the desired term of the agreement (for recurring projects, such as regional needs and assets reports, a timeframe covering multiple cycles of data collection is recommended).
- identification (if known) of any collaborators who will be collecting data, including changes to the collaborators.
- information on how the data will benefit the tribe, Arizona’s early childhood system, and FTF.

A data collection agreement for a regional needs and assets report or formal study specific to a single region should also include language providing that:

- the tribe will have the opportunity to provide feedback on a draft report or other write-up prior to publication to ensure compliance with the data collection agreement. The tribe may indicate its preferred method of receiving the information, such as an in-person, virtual presentation, or written report.
- the tribe will complete its review and provide any feedback within a set time period, usually 30 days, and FTF may publish the information if no questions or concerns have been raised or if they have been resolved.
- FTF and the tribe will enter into a consultative process in situations where the tribe has ongoing questions or concerns regarding the information in order to resolve those issues and support FTF in preparing the information for publication.
- Once FTF has received tribal approval to publish the information, additional tribal approval is not required for future publications using the same information (i.e., publications not specifically listed in the agreement) unless FTF completes additional data analysis or draws additional conclusions.

A data collection agreement relating to a needs and assets report or formal study that is statewide or multiregional should address, as appropriate, how the findings will be shared with the tribe, what opportunity for feedback may exist, and FTF's ability to publish the report or study.

FTF should only need to amend a data collection agreement if FTF desires to collect additional data or complete additional data analysis not identified in the agreement.

Once a data collection agreement is in place, FTF will provide the tribe with a principal point of contact for all communications and requests associated with the tribally protected data collection covered by the agreement. FTF may also request the tribe to provide a principal point of contact for the same purposes.

FTF will keep data collection agreements as long as it continues to house data collected under the agreement.

A tribe may request a copy of the collected data from FTF, and the data collection agreement should explain how a tribe can make that request. Additionally, if FTF plans to destroy or delete any primary data collected under a data collection agreement, FTF should contact the tribe to ensure the safe and efficient transfer of any data to the tribe prior to completing the destruction. FTF will not, however, transfer data in violation of the law or transfer confidential personally identifiable information except where required by an IRB or a data collection agreement or allowed for research purposes under FTF's Data Security Policy.

Data Sources–Definitions

FTF and its collaborators collect data from three sources: primary, secondary, and tertiary.

Primary data collection refers to FTF or an FTF collaborator obtaining data directly from individuals on tribal lands, with the individuals' consent. Examples of primary data collection include program administration and implementation, informal surveys, interviews, and formal studies.

Secondary data collection refers to two situations. Secondary data collection refers to FTF or an FTF collaborator obtaining a copy of data collected by another organization, such as a tribal department or entity, the federal government, or another state agency. Secondary data collection also refers to FTF accessing data already obtained from the tribe and which has not previously been published, as permitted by any appropriate tribal approvals.

Examples of secondary data include census records (federal government), school enrollment information (Arizona Department of Education), the number of births (Arizona Department of Health Services or tribal enrollment department), the number of child care centers (tribal Head Start department), and the number of young children with recommended vaccines (IHS, 638 health service facility or AHCCCS). Usually, the data for needs and assets reports comes from secondary data collection.

Tertiary data collection refers to accessing data already obtained from the tribe and which has previously been published (e.g., reports and policy briefs).

Data Sources–Protocols

Primary data collection

In the case of primary data collection of tribally protected data for a needs and assets report or for a formal study, FTF or an FTF collaborator will take the following steps:

- Provide the tribe with the name of the FTF collaborator responsible for collecting the data and the collaborator's data collection timeframes, and if any questions or concerns with the identified collaborator arise, FTF will work with the tribe in a consultative process.
- Advise individuals giving data that the personally identifiable information they provide is confidential, that they may withdraw from participation at any time prior to the completion of data collection activities, and that if they withdraw the information obtained from them will not be used in the report or study. This is often done within a Consent Form that participants sign.
- Give careful thought to cultural considerations around the data collection approach, including the language of data collection tools either selected or created as well as the use of a variety of data collection modalities.

- Potentially involve FTF staff and the regional partnership council in the selection or creation of data collection tools and in the selection of the collaborator where the report or study is specific to a region.

Secondary data collection

For secondary data collection of tribally protected data, FTF will determine and follow the process or protocol for requesting data from the tribe or organization with the data (e.g., ITCA). If required by the organization's process or protocol, FTF will ask the tribe for evidence that FTF has the tribe's permission to access the data. While FTF and its collaborators may receive secondary data in individual-level or aggregated form, FTF will only publish tribally protected secondary data in aggregated form.

FTF may wish to include the number of individuals or child care providers served by an FTF-funded program or service in a needs and assets report. For example, this may include the number of child care providers participating in Quality First, the number of participating providers with a 3-5 star rating, the number of children enrolled at Quality First child care providers, the number of children enrolled at providers with a 3-5 star rating, the number of children receiving Quality First scholarships, and the number of families receiving home visitation. FTF may share the number served with an FTF collaborator that is collecting data for the needs and assets report and include those numbers in the report subject to FTF's Data Suppression procedures.

Tertiary data collection

FTF will only republish tertiary data that was tribally protected data at the time FTF first collected it, in its previously published format, without additional data analysis or conclusions, unless FTF obtains tribal approval to republish the tertiary data in a different format or with additional analysis or conclusions, as applicable.

Publicly available data collection

In some cases, particularly for needs and assets reports, FTF or its collaborator collects publicly available data related to individuals living on tribal lands from sources such as the U.S. Census Bureau, the Arizona Department of Education, the Arizona Department of Health Services, and the Arizona Department of Economic Security. For example, publicly available data includes information available on public websites, including a tribe's website, as well as unpublished information that members of the public may obtain upon request without needing tribal permission. If FTF or its collaborator will collect and use publicly available data in addition to tribally protected data for a needs and assets report, FTF should notify the tribe about the kind of publicly available data that FTF or its collaborator will collect. This notification should typically occur at the same time as seeking approval to collect tribally protected data. If FTF or its collaborator will collect and use only publicly available data for a needs and assets report, then no notification is necessary.

Data Analysis

FTF Research and Evaluation staff will analyze data or will review and approve an analysis by an FTF collaborator.

For secondary data, FTF or its collaborator will work with each of the data source organizations to obtain the calculation or methodology behind the accessed data to ensure FTF's analysis plan and interpretation of the data is accurate. This will safeguard the integrity of the data presented in its final format, as well as what is shared with tribal leaders, regional councils, the FTF Board, and stakeholders.

In addition, FTF Research and Evaluation staff will consult with FTF Tribal Relations staff and regional staff in order to take culturally sensitive approaches to handling data elements. FTF Tribal Relations staff and regional staff should also work with collaborators to help them take culturally sensitive approaches to handling data elements too.

Data Protection–Security

FTF has the right to store all tribally protected data collected and to use that data consistent with this Tribal Data Policy and individual data collection agreements or other tribal approvals. FTF will securely store tribally protected data in the FTF Secure Data Storage System per FTF's Data Security Policy.

In accordance with the FTF Data Security Policy and FTF Collaborator Data Policy, FTF staff and collaborators must ensure that all tribally protected data in their personal possession is kept secure at all times against unauthorized or unlawful loss or disclosure.

Data Protection–Limitations on Release

FTF will only release tribally protected data in accordance with this Policy, the FTF Data Security Policy, the FTF Collaborator Data Policy, and any applicable data collection agreement.

FTF intends to avoid any possibility of inadvertently reporting personally identifiable information. While FTF uses aggregated data in its reporting, there are some cases where specific populations may include only a few individuals. In such cases, FTF will enforce the FTF Data Suppression procedures found in the FTF Data Security Policy and the FTF Collaborator Data Policy.

FTF will only publish a story or quote of an individual living on tribal land in anonymity or with consent from the individual to use the individual's name.

FTF may share personal information about an individual living on tribal land who is participating in an FTF-funded program or service with another state agency for program compliance purposes, including determining whether an individual applying for a Quality First child care scholarship is already receiving

child care assistance from the Arizona Department of Economic Security (DES), if FTF has consent from the individual.

FTF will not share tribally protected data without the appropriate tribal approvals, unless the data is being shared as described in this Policy or as required by law. In the case of sharing with a collaborator or other entity for a joint project, FTF will require the collaborator or other entity to follow the confidentiality and publication provisions of this Policy as well as any applicable requirements in a tribal data collection agreement.

Publication–Tribal Review

For regional needs and assets reports and formal studies specific to a single region, if required by a data collection agreement, tribes will receive information on tribally protected data collected and conclusions drawn by FTF in draft format prior to publication of the data to ensure compliance with the agreement. Tribes have the discretion to identify a preferred format in which FTF should present the draft information to the tribe (e.g., in-person presentation or written report). FTF will cooperate with tribes to establish suitable reporting and review opportunities.

The data collection agreement should stipulate a timeframe by which the tribe will complete its review, usually 30 days, and indicate that FTF may publish the information if no questions or concerns have been raised or if they have been resolved. FTF and the tribe will enter into a consultative process in situations where the tribe has ongoing questions or concerns regarding the information, in order to resolve those issues and support FTF in preparing the information for publication.

Publication–General

In this Policy, publication refers to disseminating materials in a printed or electronic format for public distribution (e.g., needs and assets reports, impact reports, fact sheets, annual reports). Publication does not include distributing the materials to those responsible for or involved with collecting, storing, analyzing, preparing, or approving the data or materials. Additionally, FTF regional council members may participate in the review, discussion, and presentation of tribally protected data and materials based on the data, including data and information publicly displayed on a screen, at their public regional council meetings prior to publication, without handing out copies of tribally protected data and materials to the public.

FTF and its collaborators may use all collected data in aggregated form (not personally identifiable) at the regional, county, or state level in a variety of public formats, including, but not limited to: reports and policy briefs, web pages, and marketing materials. Although data collection agreements should list the specific products in which FTF and its collaborators will use the data or material based on the data, FTF reserves the right to use that data and material in future publications not listed in the data

collection agreement as long as the new publication does not involve additional data, analysis or conclusions.

In addition, as a public entity, the work of FTF is subject to state public records law. All final work products—including any materials published by FTF—are subject to public records law and must be made available for inspection upon request by any member of the public as required by that law.

Tribal Access to Data

Tribes may officially request copies of collected data from FTF by submitting the FTF Tribal Data Request Form (incorporated below). The form allows tribes to easily request data for specific FTF activities. FTF will work with a tribe to provide the data in a mutually agreeable format (e.g., Word or Excel). FTF will not, however, provide data in violation of the law or provide confidential personally identifiable information except where required by an IRB or a data collection agreement or allowed for research purposes under FTF's Data Security Policy.

FTF's Data Security Policy and Collaborator Data Policy may be viewed on the FTF website at <http://www.firstthingsfirst.org/grants/grantee-resources>.

FIRST THINGS FIRST TRIBAL DATA REQUEST FORM

Data Requester:

Name of Person Requesting Data: _____

Tribal Affiliation: _____

Contact Address: _____

Contact Telephone/Email: _____

Preferred Data Format: _____

Example: Excel file, data tables of key variables from the report

Data Requested:

Data Collected as part of Needs & Asset Reports

- Name of data topics: Health; Family Support, Coordination; Early Learning
- Which agency data—DHS, IHS
- Current vs. historical data—Report Cycle

Example: Oral health data collected from IHS for 2024; WIC data from ITCA for 2024.

Other Data — please specify

Example: Quality First Rating and Enrollment data; FTF Quality First Child Care Scholarships data for SFY 2024

Request Instructions

Depending on the nature and format of the data being requested, formal documentation from the tribe (such as a letter/resolution from the tribal government) may be required before FTF can release data. Requests will be assessed on a case-by-case basis, and the requester will be notified of any tribal documentation required prior to release.

The requester must specify data they are requesting. FTF Tribal Relations and/or Research and Evaluation staff may contact the requester to clarify the request. Any changes to the request based on this contact will be documented in follow-up correspondence with the requester.

FTF will not provide data while collection, quality assurance and analysis activities are taking place. Only final data that has been reviewed for accuracy and integrity will be shared with the designated person of contact in the agreed upon format.

Please fill out the form and send it to:

First Things First
ATTN: Tribal Relations
4000 North Central Avenue, Suite 500
Phoenix, AZ 85012

For questions regarding this form (or to submit the request electronically), please contact:
cahunter@firstthingsfirst.org.



State of Arizona

Access Agreement

I have been made aware and understand that applicable State of Arizona statutes*, rules, policies and directives bind all State of Arizona (State) employees, contractors, vendors, volunteers and other users who have access to the State's technology systems and applications.

[State of Arizona employees] This agreement does not create a contract for employment between any employee and the State. Nothing in this agreement changes the fact that all uncovered employees of the State are at-will employees and serve at the pleasure of the appointing authority.

[Non-State employees/other users (such as, contractors, leased employees, vendors, volunteers, etc.) Nothing in this agreement creates an employment relationship with the State of Arizona.

In consideration for access to State information technology systems and applications, I agree to at all times abide by all applicable Arizona State statutes, rules, policies and directives, and understand that I am prohibited from violating the foregoing, which includes, but is not limited to, the following actions:

1. Revealing data to any person or persons outside or within the agency who have not been specifically authorized to receive such data.
2. Attempting or achieving access to data not germane to my mandated job duties.
3. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts without appropriate authorization.
4. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts for direct or indirect personal gain or advantage.
5. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts maliciously or in retribution for real or imagined abuse or for personal amusement.
6. Unauthorized access, modification or destruction of any computer, computer system, State information system, hardware appliance, network device, media device, computer program, data structure, database, or program code or script.
7. Unauthorized installation or connection of any computer or electronic equipment to a State network.
8. Recklessly disrupting or causing disruption of any computer, computer system or State information system.
9. Unauthorized use of electronic messaging or other communications.
10. Using State equipment or property, including equipment or property leased to the State, for other than work related purposes, unless authorized by written agency policy or other proper authorization.
11. Using a personal device that is not protected with approved and up-to-date anti-virus software and fully patched to access any State of Arizona network.

12. Removing sensitive data from the State network or State devices that are not fully protected with encryption.
13. Using another person's personal data access control identifier (USERID) and password.
14. Revealing my personal data access control identifier and/or password to another person.
15. Asking another user to reveal his/her personal data access control identifier and/or password.
16. Accessing, copying, disclosing, or deleting personally identifiable information, personal health information or other sensitive non-public information beyond that authorized by statute or specific authority of authorizing agent.
17. Accessing, copying, or disclosing critical information technology infrastructure information without authorization.
18. Using software on the local area network (LAN), or on any PC in any manner other than in accordance with the license agreement.
19. Making, acquiring, using, or distributing unauthorized copies of computer software.
20. Bringing in software (from outside the Agency) for use on the LAN or PC without the prior written permission of my Supervisor, Agency Authorizing Authority/Designee and unit responsible for Information Technology.

[State of Arizona employees] All new State employees must be provided with a copy of A.R.S. § 38-448 at the time of authorizing an employee to use an agency computer; the full text of this statute appears below:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

A. Except to the extent required in conjunction with a bona fide, agency approved research project or other agency approved undertaking, an employee of an agency shall not knowingly use agency owned or agency leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sexual acts as defined in section 13-3501. Agency heads shall give, in writing, any agency approvals. Agency approvals are available for public inspection pursuant to section 39-121.

B. An employee who violates this section may be subject to discipline or dismissal.

C. All agencies shall immediately furnish their current employees with copies of this section. All agencies shall furnish all new employees with copies of this section at the time of authorizing an employee to use an agency computer.

D. For the purposes of this section:

- 1. "Agency" means:*
 - (a) All offices, agencies, departments, boards, councils or commissions of this state.*
 - (b) All state universities.*
 - (c) All community college districts.*
 - (d) All legislative agencies.*
 - (e) All departments or agencies of the state supreme court or the court of appeals.*
- 2. "Information infrastructure" means telecommunications, cable and computer networks and includes the internet, the world wide web, usenet, bulletin board systems, on-line systems and telephone networks.*

I agree to seek clarification before entering, modifying, deleting, altering, or disclosing data. I agree to

immediately notify my supervisor, manager or any member of the Agency's executive team of any suspected or confirmed unauthorized disclosure or misuse in violation of this agreement or any applicable statutes, rules or policies.

Appropriate action will be taken, including immediate termination of access, to ensure that applicable federal and state statutes, regulations and directives governing confidentiality and security are enforced. Aside from revocation of access, breach of procedures pursuant to this policy or misuse of State property including computer programs, equipment and/or data, may result in prosecution in accordance with any applicable provision of statute, including Arizona Revised Statutes (A.R.S.) Section 13-2316, for computer tampering and/or:

- [State of Arizona employees] I may be subject to discipline or separation.
- [Non-State employees/other users] Violating federal and state statutes and rules, statewide policies, and agency policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring of entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.

During all times that I have access to State information technology systems and applications, I accept responsibility for adhering to all applicable State of Arizona statutes, rules, security policies and directives and agree to abide by this agreement. I understand that I have access to instruction on and access to applicable statutes, rules and policies. Failure to accept the terms of this agreement will mean I will not be permitted access to State of Arizona produced media, data, computer equipment and software.

Print Name _____

Agency _____

Signature _____

Date _____

*Applicable State of Arizona statutes and policies include, but are not limited to:

- A.R.S. § 41-3504. Powers and duties of the department; violation; classification
- A.R.S. § 41-3507. Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure
- A.R.S. § 13-2316. Computer tampering; venue; forfeiture; classification
- A.R.S. § 41-151.12. Records; records management; powers and duties of director; fees; records services fund
- A.R.S. § 41-1750.01. National crime prevention and privacy compact
- [State of Arizona employees] A.R.S. § 38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions
- Statewide Policy 8280: Acceptable Use and corresponding agency policy