FIRST THINGS FIRST

Data Security Policy

Purpose

The First Things First (FTF) Data Security Policy describes how FTF protects confidential and limited distribution data from inappropriate access, use, modification, or disclosure. This Policy is supplemented by these separate data policies:

- FTF Tribal Data Policy
- FTF Collaborator Data Policy

Background

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.

Under state law, FTF must identify and report on the assets available for these programs and the unmet need for these programs statewide and in each individual 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 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 statewide and in each region of Arizona.

Policy

FTF collects data and other information about private organizations, government entities including tribal entities, early childhood professionals, and children and families for two primary purposes, which are related to the provision of programs and services either for young children and families or for early childhood professionals:

- needs and assets reports
- program and service administration and implementation

[1] A.R.S. §§ 8-1161(A)-(C) & 8-1192(A)(1)
[2] A.R.S. §§ 8-1151(B)(6), 8-1174 & 8-1192(A)(4)

Occasionally, FTF may also collect data and other information for other purposes, including systems change projects, using informal surveys, formal studies, or other informal and formal approaches.

FTF often collects data through collaborators, which include grantees (i.e., grant partners), governmental entities, and vendors (i.e., contractors) 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 ("collaborators").

In this Policy and in the supplemental Tribal Data Policy and Collaborator Data Policy, 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).

FTF will store, process and transmit confidential and limited distribution data as summarized here and further explained below. FTF will protect and secure confidential and limited distribution data throughout its lifecycle, as well as any FTF information system that stores, processes or transmits that data, in a reasonable and appropriate manner for a public agency handling program, quality improvement and research data.

FTF will not publish or otherwise disseminate data in violation of law. Furthermore, FTF will not disseminate confidential, limited distribution, or tribally protected data for any purpose other than those noted in this Policy, the Tribal Data Policy, and the Collaborator Data Policy. If FTF enters into a contract with a collaborator to collect data or perform data reporting or statistical analysis, that contract will require the collaborator to protect confidential, limited distribution, and tribally protected data as described in the Collaborator Data Policy as well.

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.[3]

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, below.) Limited distribution data may be subject to HIPAA, FERPA, tribal law, or other data regulation.[4]

[3] *See also* ADOA-ASET Policy 8110 ¶ 6.2.1 (giving examples of other types of confidential data).
[4] For the purposes of ADOA-ASET Policy 8110, limited distribution data is a form of confidential data.

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 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 the 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 and the Inter Tribal Council of Arizona. Tribally protected data does not include publicly available data from any source.

Protecting Confidential Data by Sharing Non-Personally Identifying Data

Aggregated Data

FTF may use confidential data to produce aggregated data reports. Aggregated data is data that has been combined or summarized from individual records to show overall trends or patterns, rather than details about specific individuals. In general, this aggregated data is public data even if the non-aggregated source material is confidential. In some cases, however, specific populations include only a few individuals; this creates a risk that even aggregated data for those populations will permit the identification of individuals. In those cases, the aggregated data for those populations becomes limited distribution data. FTF will suppress this aggregated limited distribution data in publications in accordance with the "Data Suppression" section below. This limited distribution data may also be protected by contract or suppressed in other disclosures.

Data Suppression

Confidential or limited distribution data must not appear in publications. When a publication includes aggregated data, FTF will suppress any limited distributed data. The statistical cutoff procedures help ensure that aggregated data does not allow the identification of any individual. FTF's intent is to avoid

the possibility of inadvertently reporting personally identifiable information associated with confidential and limited distribution data.

For data related to social service and early education programming, limited distribution data refers to counts of fewer than ten, excluding counts of zero (i.e., all counts of one through nine). Examples of social service and early education programming include the number of children served in TANF, AzMerit scores and the number of children served with an IEP or IFSP.

For data related to health, limited distribution data refers to counts of fewer than six, excluding counts of zero (i.e., all counts of one through five). Examples of health data include preterm births and births to mothers using tobacco during pregnancy.

Handling Specially Protected Confidential Data Types

Tribally Protected Data

Third parties will not access or use tribally protected data except in accordance with the FTF Tribal Data Policy. Where the Tribal Data Policy permits access or use of that data, then this Data Security Policy including the "Providing Others with Access to Data" procedures below and the Collaborator Data Policy further limit access and use of that data. The "Providing Others with Access to Data" procedures also apply to non-tribal data.

HIPAA & FERPA

FTF sometimes receives or collects information covered by HIPAA or FERPA. HIPAA- and FERPA-protected information may include data such as first name, last name, address with zip code, date of birth, and social security number. FTF will protect HIPAA- and FERPA-protected data as required by those laws and will not share that data with collaborators, the public, researchers, or tribes unless permitted by HIPAA and FERPA, as applicable.

Sometimes HIPAA and FERPA protected data is used for the purpose of identifying a child or parent to ensure it is the same individual(s) over time. In these cases, the individual-level data will be aggregated and integrated with information from other agencies to provide trend, usage and impact information over time. FTF's intention is to use this personally identifying information to match data sets to individuals and not to report on the personally identifying information.

Financial Data

FTF may use its system interface to capture and communicate information relevant to monetary transactions. FTF will secure this information, its manipulation, and the subsequent internal FTF functions to varying degrees so as to assure confidence of transactions. It is also necessary to secure that information from compromise where data and associated measures could influence future decisions of FTF, its collaborators, or other interested parties.

Providing Others with Access to Data

Collaborator Access to Data

Most data contained within the FTF system that has been shared or entered directly by collaborators and other entities is public data. But certain data from these collaborators and other entities will only be available for viewing or manipulation by (i) FTF, (ii) the individuals, collaborators and other entities to whom that data pertains, and (iii) those individuals, collaborators and other entities identified as germane by FTF.

FTF may share personally identifying information with another government agency where that information is necessary to link data held by FTF to data held by the other agency. Additionally, where FTF is one of multiple collaborators and other entities jointly working on a specific project, FTF may share confidential and limited distribution data collected as part of the project with those collaborators and other entities. FTF will not share, however, tribally protected data for these purposes without the appropriate tribal approvals, unless the data is being shared as described in the FTF Tribal Data Policy or as required by law. In any circumstances of sharing, the collaborator or other entity must agree to follow FTF's Collaborator Data Policy and Tribal Data Policy, if applicable.

Public Access to Data

FTF will provide the public with access to public data but not confidential or limited distribution data, in accordance with Arizona's Public Records Laws.

Researcher Access to Data

FTF recognizes the importance of availability of Arizona early childhood data to researchers. FTF will provide researchers with access to public data, following a request, in accordance with Arizona's Public Records Laws.

When researchers request access to nonpublic data, FTF will work with the researchers with the goal that they will receive the most meaningful data possible while ensuring that information will not be disclosed to the public that could be used to identify individuals to whom the data relates. FTF will also work to ensure that researchers do not misuse data by drawing and publishing conclusions not supported by the data or by using data contrary to the conditions that were placed on FTF's ability to collect and use the data, like for tribally protected data. Researchers will not have access to tribally protected data unless the tribe gives approval.

Researchers' request for access to confidential or limited distribution data must explain the purpose of the research study; identify any facts, if applicable, that demonstrate that FTF authorized the study or that the study is being conducted on behalf of FTF; and explain how they will ensure data confidentiality and security. FTF will require each researcher to sign a detailed data use agreement before receiving access to the data. The data use agreement will define the data covered by the agreement and will set out how the data will be stored, accessed, used, maintained, disseminated, and destroyed. FTF will also require researchers to supply FTF with a copy of any analysis or report created with the data and to destroy their copies of the data once they complete their research. FTF will consider researchers' requests on a case-by-case basis.

It is anticipated that FTF will share data containing personal identifiers with researchers only in very limited cases. In those instances, any release of data to researchers will be considered a loan of data; i.e., the recipients will not have ownership of the data. Prior to sharing data containing personal identifiers, FTF will require documentation and evidence of the researchers' physical and process security standards meeting or exceeding FTF's security standards. FTF will not send data containing personal identifiers via email, webmail, web browser, peer-to-peer network or wireless transmission; the preferred method of transmittal is through an established secure web service or secure FTP (File Transfer Protocol) site via the internet.

Tribal Access to Data

Tribes may have access to data collected from children and families living on their tribal lands and early childhood professionals working on tribal lands in accordance with the Tribal Data Policy, "Tribal Access to Data" section.

Data Security & Protection Measures

Network Access and Firewall Protection

FTF's network security standards will ensure secure and seamless interconnection of communications networks and systems, while protecting FTF's physical infrastructure, computing resources, and data storage, as outlined in this section.

These security standards will be implemented through both FTF's internal network infrastructure and the state's AZNET program for network communication services. FTF will utilize multi-layered protection at the internet gateway, network server, and desktop levels to prevent the introduction of malicious code or unauthorized access into its information systems. All external (inbound and outbound) traffic will be routed through secure firewalls, which will feature security logging capabilities. Individual firewalls deployed across FTF's systems will be centrally administered and managed to ensure timely application and updates of security measures.

FTF will use a web service—via standardized XML messaging or other formats—to receive, collect, or exchange data with other web services. FTF will route all external connections to its networks through secure gateways and protect them using encryption. FTF will employ Secure Socket Layer (SSL) technology between web servers and browsers to authenticate both the server and the user's browser. FTF will maintain an inventory of all external individuals, collaborators, and other entities with active connections to FTF systems via web services. When a connection is no longer needed, FTF will promptly disable it and remove associated key network components to prevent inadvertent reconnection.

Physical Storage Security

FTF will safeguard the physical housing unit of electronic data, including following these physical security practices:

- Locate in secure locations, lock, and restrict access to FTF's information systems (servers, storage, client devices, etc.), media storage areas, and related communication wiring and network devices to authorized FTF personnel only.
- Monitor access to critical data or information storage areas by establishing the identity of the person entering/exiting as well as the date and time of the access (e.g., recording badge information, videotaping) and by providing data for auditing physical access.
- Use locking mechanisms with security ID badge or security ID badge and key access to access secure areas. The Operations Unit may change the access codes periodically.
- Prohibit "piggybacking" of badge holders where FTF employs badge-reading systems to log access into and out of a secure facility.
- Secure unused keys, entry devices, etc.
- Control physical access to "critical" IT hardware, wiring and network devices on a restricted/least privilege basis for the authorized employee or contractor to complete assigned tasks.
- Employ back-up systems/servers physical access security measures equivalent to those of the primary system.

- Protect information systems, media storage areas, and related communication wiring and network devices against loss or malfunction of environmental equipment or services necessary for the operation of the facility.

Theft or loss of IT equipment may potentially result in the unintentional disclosure of confidential or limited distribution data, therefore FTF will password protect and routinely inventory, account for, and safeguard its computing and telecommunications equipment from loss and resulting unauthorized use. FTF will also consistently control and label removable storage media (disk, tapes, CDs, etc.) to guard against misplacement and loss or unauthorized use.

Data Handling

FTF will practice physical safeguards for workstations to restrict access to authorized users, including:

- Password protecting all workstations.
- Positioning computer monitors so that visitors or unauthorized persons cannot easily view the screen or what is displayed.
- Prohibiting unsupervised access by visitors to areas where FTF houses workstations with access to confidential or limited distribution data.
- Recording each laptop given to an employee.
- For employees who maintain or have access to confidential or limited distribution data, keeping their laptops within their control while outside the facility.
- Immediately reporting a lost, stolen, or damaged laptop to a database administrator or designee.

Staff must keep secure all confidential and limited distribution data in their possession at all times against unauthorized or unlawful loss or disclosure. This includes complying with the following procedures for both confidential and limited distribution data:

- Store confidential and limited distribution data held on computers and computer systems in line with FTF data security policies.
- Keep paper files and other physical records or documents containing confidential and limited distribution data in a secure physical environment.
- Keep hand-carried confidential and limited distribution data with an authorized staff member and protected from unauthorized disclosure.
- Turn over or put out of sight confidential and limited distribution data where unauthorized individuals are present.

- Do not move confidential and limited distribution data without authorization outside of a controlled area or an authorized employee's physical control.
- Do not leave confidential and limited distribution data unattended, even temporarily, outside of a controlled area or an authorized employee's physical control.
- Do not discuss confidential and limited distribution data in the presence of unauthorized individuals.
- Correctly secure confidential and limited distribution data if transmission of the data is necessary.
- Correctly dispose of confidential and limited distribution data.

Staff must not store confidential or limited distribution data from, or to be placed in, the Secure Data Storage System on portable devices (such as laptop computers, digital cameras, tablets, smartphones and portable hard drives including flash drives, USB memory sticks, or similar storage devices).

FTF will only transmit confidential or limited distribution data in the Secure Data Storage System using secure, encrypted formats, ensuring user IDs are stored/transported separately.

All FTF staff also sign and must abide by the state's technology systems and applications Access Agreement (Attachment A).[5]

Secure Data Storage System and Architecture

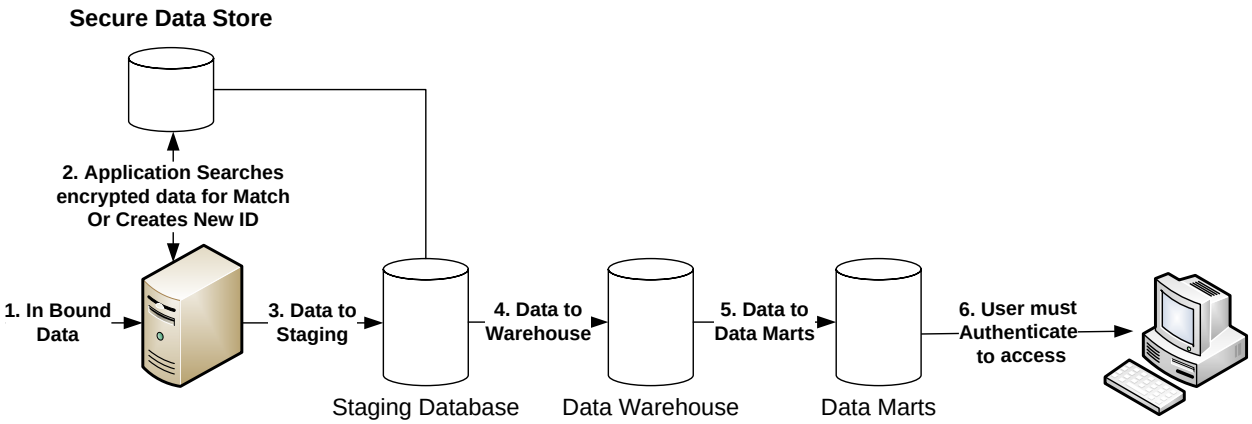
FTF will use a data system model with separate, encrypted storage of confidential and limited distribution data. FTF will encrypt the secure data storage and associated backups using Microsoft's SQL 2014 built-in functionality for creating certificates along with encryption and decryption functions to provide a secure solution. FTF will use Field Level Encryption, with encryption being performed with certificates controlled by a separate group than FTF database administrators.

FTF will store confidential and limited distribution data in the Secure Data Storage System in a secured SQL data file. FTF will encrypt and store the data file using the binary data type format. FTF will store user IDs separately for those who encrypt and those who decrypt. Only those employees identified as need to know and who are authorized will have access to the information. FTF will encrypt the keys for decryption as well and store them in a separate database from the actual data.

Figure 1 shows the high-level architecture of the confidential and limited distribution data model used at FTF.

[5] ADOA-ASET Form F8280.

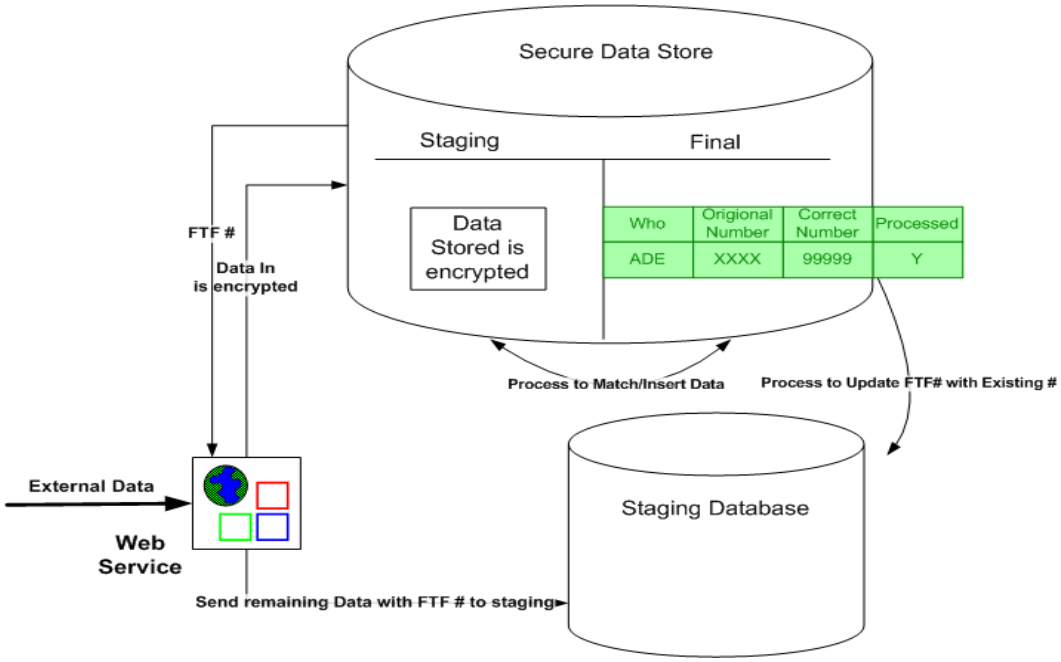
Figure 1: Architecture of Secure Data Store



Confidential and limited distribution data entering the Secure Data Storage System will do so via one of two paths: externally through a secure web service or FTP site and internally through the data collection system built by FTF. Once a user enters and requests to save the data, the data will be sent to the Secure Data Store. FTF will record complete audit trails of every access regardless of the user.

Figure 2 provides an overview of FTF's secure data storage and encryption process.

Figure 2: Secure Data Storage and Encryption Process



Staff Access to Secure Data Storage System

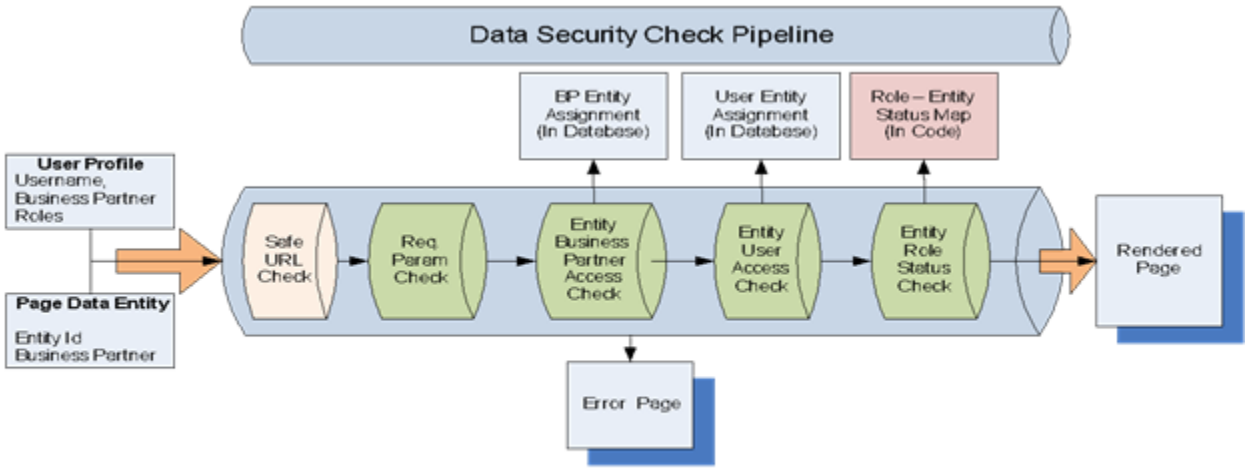
FTF will provide staff with access to data resources in the Secure Data Storage System on a least privilege basis, that is, the minimum set of resources required for their role. FTF will maintain a record of electronic access to all data identified as confidential or limited distribution in the Secure Data Storage System. This will serve to improve accountability and minimize the impact of any security violations.

FTF will inform its information technology (IT) personnel, as well as other business units with necessary access to confidential or limited distribution data in the Secure Data Storage System, about the security policies and procedures for confidential and limited distribution data. FTF will use practices such as separation of duties, when required or feasible or both, to ensure that personnel authorizing access to data in the Secure Data Storage System are distinctly separate from those who authorize and give physical access to Secure Data Storage System areas and equipment. The CEO or COO may authorize access to confidential and limited distribution data, and database administrators will grant physical access.

Collaborator Authentication and Authorization

In order to provide collaborators and other entities with limited access to shared data and certain financial information, the FTF Secure Data Storage System will use a mechanism of authentication (identifying who they are) as well as authorization (identifying permissions and access levels) for those who come to the FTF site. Both standard forms of authentication via username and password and authorization via identity management are conducted using Active Directory. Figure 3 depicts FTF's process that employs three checks for authentication and authorization of all users.

Figure 3: User Authentication and Authorization using Active Directory



Breach

An important aspect of FTF data security policies is the effective and timely reporting of all suspected incidents of misuse or loss of confidential or limited distribution data or breaches of data security. FTF will promptly identify, report, manage, and provide notification of a data breach related to an information security incident.

In the event a security breach occurs, FTF staff should implement the following steps:

1. Shut down the breached data systems identified immediately and take them off the network.
2. Identify the extent of the data accessed.
3. Immediately notify the IT Director of the breach and the extent of the breach.
4. Come up with a communication plan regarding the breach, if deemed necessary. The IT Director will work with the CEO, COO, Chief Data Officer, and Chief Public Affairs Officer to come up with the plan. The Chief Tribal Relations Officer will be involved too if the breach involves tribally protected data.

FTF must also:

5. Notify the Arizona Department of Administration's Arizona Strategic Enterprise Technology Office (ASET) within 1 hour of the breach.
6. Notify all individuals, organizations, and entities whose data was breached; in the case of children, notify their parent or guardian.
7. Clean and secure any suspect component of the IT infrastructure before bringing the component back on line.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privilege and employee discipline or termination. Violators may be subject to criminal charges as well. *See* Attachment A – State Access Agreement.

Exceptions

The CEO may approve exceptions to this Policy. Changes to a data agreement, however, may only occur with consent of both parties to the agreement.

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