Comprehensive Data Management Policy

Policy Number: AD1701-15	Board Approval Date: 5/2017	Policy Council Approval Date: 4/2017

PERFORMANCE OBJECTIVE: A program must design and implement program-wide coordinated approaches that ensure the management of program data in areas such as quality of data and effective use and sharing of data, while protecting the privacy of child records in accordance with applicable federal, state and local laws. The program will establish procedures to effectively support the availability, usability, integrity, and security of data, and have them approved by the governing body and policy council. (Part 1302.101)

OPERATIONAL PROCEDURES::

General Information about data collection and management

- A variety of electronic and paper data will be produced and collected by the operation of the program. This might include (but is not limited to) data that are: observational, raw, physical collections, curriculum materials, images and videos.
- Family or participant eligibility data will be collected when an applicant initially expresses interest in the program. After enrollment, a diverse number of assessments and progress reports will be conducted, documented and entered into physical files or electronic databases.
- Child tracking data that is collected pursuant to the operation of the program will be stored in the ChildPlus data base. Participant eligibility documentation and additional family information such as home visit documentation will also be stored in ChildPlus and in paper files.
- Additional child assessment data is collected and entered into web-based software such as Kindercharts, SurveyPro, LifeCubby and TS Gold.
- Quality control measures will include a system that ensures 100% of participant files will be checked during the data entry process. In addition, the ERSEA *(Eligibility, Recruitment, Selection, Enrollment and Attendance)* Coordinator conducts an additional review of all income-related information to ensure participant eligibility.
- The effective use of and quality of data is also regularly inspected as part of the program's ongoing monitoring system and file review process.

Backing Up Data And Data Products

- ChildPlus hosts the program database on a secure cloud server.
- ChildPlus experts perform all the archiving, upgrades, and maintenance for the program.
- All of ChildPlus data is kept on secure, encrypted cloud servers that are monitored 24 hours a day, 7 days a week.
- ChildPlus creates backup copies of the data every week. Incremental backups are performed each night to minimize the impact of any catastrophic hardware failure that might occur.
- The full physical backups are moved offsite once per week to be archived so that databases can be restored to any point in time.
- The cloud hosting provider is Rackspace. Rackspace is a state-of-the-art managed hosting facility with a zero downtime network and a 1 hour hardware replacement guarantee.
- Secure Server Details

    - SAS70 Type II certified hosting provider.
    - Keycard & biometric scanning access control.
    - CISCO firewalls & Intrusion Detection Systems.
    - 128-bit SSL encryption – same level of security as banking websites
    - Monitored 24 hours a day, 7 days a week.

Security & Protection Of Data And Data Products

ChildPlus, the primary data software used, has multiple, customizable security settings that are used by the program.

- Tiered level user access which gives the program complete control over who has access to what data and how that data can be used.
    - Create and assign permission and privilege levels for individual users and user security groups.
    - Permissions can be set down to the individual field level.
    - Unlimited security groups can be created to precisely control access for groups of staff.
    - User security groups can be full, view only, or restricted access.
    - Access can be limited by specific classroom to multiple centers.
- Password Policy Enforcement
    - Forces the user to change their password the first time they log into the system.
    - Requires the user to change their password after a prescribed time period.
    - Sets a required weakness or strength for passwords.
    - Lockout users after a specified number of consecutive failed login attempts.
    - Sets a customized inactivity timeout.
- Safeguards are in place for accurate and complete data entry.
    - Set fields as required or recommended.
    - Users receive a warning when an important field is left blank.
    - Sign in/out log ensures accountability.
    - Data changes can be monitored with the Audit Log which shows a history of changes made to data.

Agency-wide Security Measures:

- Each computer has username and passwords in order to access the device.
- Each computer has a 10 minute screensaver password requirement per computer
- The Agency uses Avast Cloud Business to centrally monitor virus and malware on workstations while the servers have a locally controlled Symantec solution.
- The Agency employs Domain-Based Message Authentication, Domain Keys are identified in mail and sender policy framework to help protect email.
- All Apple devices require a PIN to access.
- A current remote monitoring system for Apple devices is in place via Meraki software. This allows for each Mac device to be enrolled via Apple Device Enrollment Program. This allows for devices to be located via GPS, remotely wiped if a device is lost, security policies enforced such as the above mentioned PIN, monitoring of what is installed; ability to limit what can be installed or removed.
- The Main Office Building and satellite offices have restricted entry protocols. Participant files are stored in locked offices or locked filing cabinets.
- In addition to the security provisions listed above, the Agency is in the process of testing/implementing three additional safeguards:

1. Two factor authentications to Gmail/google services will soon be in place Agency-wide.

2. A remote monitoring system with remote software patch management features has been approved for implementation. This can help monitor remote systems for common issues such as antivirus, malware, automate remote security issues that need to be pushed out quickly. The remote monitoring system for workstations is a bit different in functionality versus the apple system listed in the next paragraph as the windows devices have so much more capability. The software under consideration will have a 3rd party patch management solution embedded within the framework.

3. A content filtering and monitoring solution is being implemented at remote sites via a product called CDome Shield (Comodo Dome Shield). This product blocks all sites hosting malware, phishing sites, and scam sites while also blocking access to sites that contain sexually explicit material. The product offers robust monitoring via reports and restrictions. This product also integrates within the remote monitoring suite being used by the Agency.

Data Management Responsibility

The primary contact for Agency information technology operations is Travis Mitchell, Director of Information Technology and Communications – tmitchell@escswa.org.....417-781-0352

Metadata content and format

Metadata will be created and captured from other data sources. Metadata will not contain any Personal Identifiable Information. Metadata will be used for program self-assessment, data-driven decision-making, staff training and analysis/reporting to Board and policy groups. Metadata will consist of reports, charts and graphs that provide meaningful information for program operation, monitoring and planning.

Effective use, access, sharing, and re-use of data

- The program has mandatory obligations for sharing certain data. These include law enforcement requests, child abuse and neglect reporting, funding source reviews, legal action and 3rd party auditors.
- The program also seeks authorization to share information with partnering agencies and consultants. The purpose of this sharing is to provide services and meet funding performance objectives. Parents can opt out of this sharing.
- Additional information on data access, sharing and re-use can be found in the program confidentiality policy.
- Program data and information is only to be used when conducting program business.
- Program information may not be used for personal profit.
- The Agency employs data destruction technologies when disposing of equipment. Employees must not dispose of equipment themselves but must turn it in to the Director of Information Technology and Communications for secure disposal.
- Education records are protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) as amended.
- The program is allowed to disclose PII from child records without parental consent to federal or state officials, in connection with an audit or evaluation of education or child development programs, as long as the program maintains oversight of child records through a written agreement or other means.
- The program may participate in the state education data system to the extent practicable.

Long-term storage and data management protection

Archiving is about saving data over a long period of time for legal or regulatory compliance purposes.

- The Agency uses Stronghold Data for its long-term data storage. This company provides a highly-secure facility that includes the following systems:
  - An above ground guard shack and entrance
  - The data storage facility is 85 feet underground.
  - The main entrance requires key card, visible identification and biometric fingerprint access.
  - The entire facility is monitored by video cameras.
  - The data is protected by multiple battery systems including four 400Kw UPS PowerWare units. Each unit is capable of maintaining system operations in the event of failure of one or more units.
  - The data is further protected by two Cummins 3000HP diesel backup generators producing 2 Mw power each.
  - Each data room has additional security requirements and its own HVAC, power and FM200 fire suppression.
  - More info is available at https://strongholddata.com/about.
- The Director of Information Technology and Communications will identify and assess external and internal risks to the security, confidentiality and integrity of Agency data. This includes the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. Methods of detecting, preventing and responding to attacks or other system failures will be identified and implemented including procedures for responding to network attacks.
- The primary contact for archived program data is the program ERSEA coordinator. Requests for data or information about data must be forwarded to Travis Crusa – tcrusa@escswa.org....417-781-0352.

Budget
Data management and preservation costs are considered in the preparation of program budgets. Potential expenses that are considered include:

- Personnel time for data preparation, management, documentation, and preservation
- Hardware and/or software needed for data management, backing up, security, documentation, and preservation
- Costs associated with monitoring or submitting the data to an archive
- Computer repair and maintenance support.

These costs are paid from grant funds either directly charged to the grant receiving the benefit or service or charged to indirect cost when the expense and benefit are shared among multiple programs or the Agency in general.

Additional Policies
The Head Start Confidentiality Policy and the Agency Computer Usage, Electronic Mail And Security Policy both contain related requirements and guidelines pertaining to data use and privacy protection. These policies provide additional details or resources necessary to effectively use, understand and implement the Comprehensive Data Management Policy.

Enforcement
Reports of data and system compromises and the exposure of personal and restricted information should be immediately reported to a Division Director. Behavior in violation of this policy is cause for disciplinary action. Violations will be addressed as appropriate and can result in any or all of the following:

- Additional training
- Loss of computing, access or email privileges
- Monetary reimbursement to the Agency or other appropriate sources
- Prosecution under applicable civil or criminal laws
- Disciplinary actions including probation, suspension or termination

Version 1.1 5/1/17