POLICY ON AGREEMENTS INVOLVING DATA SHARING

1. Purpose. This operating procedure establishes policy to govern the development and maintenance of DCF Data Sharing Agreements as they are designed to effectively cover digital data sharing. A Data Sharing Agreement (DSA) is an agreement between a discloser of data and recipient(s) of data engaged in collaboration and development. Recipients are typically seeking data to conduct academic and or scientific research and / or to conduct business with the State of Florida. As a discloser and as a recipient of data, the Department of Children and Families (DCF) often seeks to share data with universities, other government agencies, private entities and other External Partners in furtherance of the Department’s mission, vision, and values.

2. Scope. This operating procedure applies to all Department employees and contractors.

3. Authority.
   b. Section 20.05, Florida Statutes (F.S.), "Heads of departments; powers and duties."
   c. Section 20.19, F.S., "Department of Children and Families."
   g. DHHS CMS MARS E 2.0 Requirements.
   i. Internal Revenue Service, Publication 1075, “Tax Information Security Guidelines for Federal, State and Local Agencies, Rev. 11-2016.”
   j. CFOP 5-2, “Departmental Administrative Publications System.”

4. Definitions. For the purposes of this operating procedure, the following terms shall be understood to mean:
   a. Agreement. In the context of this operating procedure, an agreement is a formal document, signed by appropriate authority from each party involved, which includes, but is not limited to, the
criteria for access to data, conditions of data use, retention of data periods, and the duration and effective date of the agreement. This type of sharing agreement can be in the form of a service level agreement, memorandum of understanding, memorandum of agreement, interagency agreement, cooperative agreement, or a data sharing or data matching agreement.

b. **Agreement Coordinator.** The representative of the DCF program office that initiates and drives a DSA internal to DCF. This role is responsible for entering DSAs proposed by their program office into DCFTracker, the tracking application used administratively by DCF to route interoffice publications for editing, review, and approval. The Agreement Coordinator will also ensure the draft DSA is distributed to the External Partner(s) for their own internal review which will be handled in turn by their own Agreement Coordinator(s). The contact information for the DCF and the External Partner(s) Agreement Coordinators must be provided within the body of the DSA and there must be at least one Agreement Coordinator listed for each participant.

c. **Chief Information Officer (CIO).** The duties of the Chief Information Officer (CIO) include the management and oversight of strategy and implementation for the usability of information technology and the business systems that support enterprise goals.

d. **Confidential Information.** Information that is exempted from disclosure requirements under the provisions of applicable state and federal law, e.g., Section 119.07, F.S., “Public Records.”

e. **Data Owner.** At DCF the Secretary of the Department is ultimately responsible for the collection, maintenance, and dissemination of DCF data. The Secretary is also the overall mission and business owner for the Department, providing the broad expression of DCF business goals and the specified target outcomes for all business operations.

f. **Data Sharing.** Transfer of digital data, between two or more parties, which may be unidirectional or bidirectional in nature. DCF may disclose its Departmental data, be the recipient of data owned by another party, or act as an intermediary in transferring data from one entity to another.

g. **DCFTracker.** The web-based tracking application used by DCF administratively to route publications for editing, review, and approval described in CFOP 5-2, “Departmental Administrative Publications System.”

h. **Director of Enterprise Data Management.** This Director of the Enterprise Data Management (EDM) team facilitates cross-departmental data sharing and assists Department data-sharing initiatives among many external entities, in addition to providing expertise and collaboration in the area of data intelligence, analytics, and reporting.

i. **Employee.** Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. Also, for the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to Department IT resources, including contracted staff and contracted vendor staff.

j. **External Partners.** The colleges, universities, other government agencies, private entities and community partners that DCF seeks to productively share data with across the state of Florida and beyond in furtherance of the Department’s mission, vision, and values.

k. **Federal Tax Information (FTI).** A term for data that consists of federal tax returns and return information (and information derived from it) that is in the agency’s possession or control, which is covered by the confidentiality protections and safeguarding requirements including IRS oversight. FTI is categorized as Sensitive and may contain personally identifiable information (PII).
l. **HIPAA.** The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. Federal law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

m. **Information and Data Custodians.** Individuals or groups at DCF that ensure the careful and responsible management of information and data belonging to the Department as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information and data custodians act as stewards, providing maximum access to information and data elements, balancing this work with the shared obligation to protect the information in accordance with the provisions of law and any associated security-related state or federal policies, directives, regulations, standards, and guidance.

n. **Information Owner.** Under the direction of the Secretary, the Director of the program office ultimately responsible for the collection, maintenance, and dissemination of a specific collection of program office information or a program area business information system.

o. **Information Security Manager.** The DCF Information Security Manager (ISM) is the person designated by the Secretary of the Department to administer the Department's information technology security program and serve as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with §282.318, Florida Statutes, and Chapter 60GG-2, F.A.C.

p. **IT Data Agreement Coordinator.** The position within the Office of Information Technology Services that is responsible for entering, maintaining, and updating completed or renewed DSAs in the OITS EDM System. These records can then be retrieved for reference and review by agency staff. The contact information for the IT Data Agreement Coordinator is provided within the body of the DSA. The Agreement Coordinator from the respective DCF program office is responsible for working with this role to provide this role with a copy of the final approved and signed DSA.

q. **Personal Identifying Information (PII).** Any information about an individual maintained by a department or agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This information is sensitive and confidential.

r. **Personal Information (PI).** Any recorded information about an identifiable individual that may include name, address, email address, phone number, race, nationality, ethnicity, origin, skin color, religious or political beliefs or associations, age, sex, sexual orientation, marital status, family status, identifying numbers, codes, symbols, fingerprints, blood type, inherited characteristics, health care history including information on physical/mental disability, educational, financial, criminal, employment history, and personal views.

s. **Protected health information (PHI).** Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

t. **System Owner.** Program office having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

5. **Guiding Principles.** DCF is committed to the goal of ensuring appropriate data handling processes to further protect the integrity, security, and confidentiality of Department data. To help ensure that DCF can continuously meet this goal, any data shared by the Department, whether received from or
disclosed to another entity, will be protected by a comprehensive written agreement that accurately describes the mechanics of the agreed-upon data sharing venture.

a. The DCF Office of Information Technology Services (OITS) actively reviews any data sharing agreements under consideration by DCF to verify appropriate data quality and security measures are in place. Within OITS the DCF ISM reviews DSAs to ensure all applicable and appropriate security controls and state and federal audit compliance controls have been effectively addressed. The EDM team in OITS reviews DSAs for content and quality control to further facilitate quality data sharing across the state of Florida.

b. Special Note. Any would-be data recipient(s) requesting federally supplied social security data in the custody of DCF must be approved by the U. S. Social Security Administration (SSA) to receive specified SSA data prior to receiving any such data through a DSA with DCF. Any DSA DCF enters into with any recipient entity / entities who have received the required SSA approval to have access to SSA data in DCF’s custody shall be required in the body of the actual Data Sharing Agreement to notify the DCF ISM and DCF CIO within one (1) hour of any detected potential breach of SSA data. The same is true of Internal Revenue Service (IRS) data entrusted to the custody of DCF; prior approval of the IRS must be obtained and it shall be required in the body of the actual DSA that the DCF ISM and DCF CIO are to be notified within one (1) hour of any detected potential breach of IRS data.

6. Procedures for DCF Data Sharing Agreement Proposals. In addition to the procedural steps outlined below, DCF employees will follow any and all other authorized DCF policies and procedures developed to better facilitate agency data sharing:

a. Legal Consultation. When a DCF program office identifies a possible opportunity for the Department and or the State of Florida to benefit from the creation and maintenance of a DSA, the respective DCF program office should first confirm with the DCF Office of General Counsel (OGC) that the data their program office owns and which is under discussion to be shared can be lawfully shared by the Department. Once that confirmation has been received, the respective DCF program office should follow any OGC guidance provided on how best to share the data in a manner consistent with Federal and State law.

b. Begin Draft Template. After conferring with Office of General Counsel, the respective DCF program office staff opting to propose a DSA should obtain a Data Sharing Agreement template (form CF 122, available in the DCF Forms) and complete a draft template.

c. Draft into DCFTracker. The DCF program office staff will use DCFTracker, as per CFOP 5-2, “Departmental Administrative Publications System,” to send a copy of their draft through a formal internal review process for both the Draft Review Phase and the Review for Signature Phase.

d. Draft Review Phase.

(1) The internal review team for draft Data Sharing Agreements at DCF must include, but is not limited to:

(a) Appropriate Program Office Management;

(b) Legal Review by OGC;

(c) OITS (Director of Enterprise Data Management’s team);

(d) OITS (DCF ISM); and,
(e) External Partner(s) (the agency / agencies or entity / entities DCF will be sharing data with as a recipient or provider).

(2) The DCF program office’s Agreement Coordinator is responsible for coordinating the review of the draft DSA by the External Partner(s). The draft DSA should be reviewed by these teams as appropriate to resolve any identified issues before moving on to the Review for Signature Phase.

e. Review for Signature Phase – OGC and Program Office. Once the draft DSA has been agreed upon and signed by the External Partner(s), the DCF program office’s Agreement Coordinator will then ensure DCFTracker is used to send their Final Draft through the Review for Signature phase. The Final Draft DCFTracker packet should be reviewed and initialed and dated first by OGC, before proceeding on to the DCF program office’s head or Designee for their signature on the DSA.

f. Review for Signature Phase – OITS and CIO. Next, the Final Draft DCFTracker packet moves to OITS where it should be reviewed, initialed, and dated first by the DCF ISM, then by the Director of Enterprise Data Management before moving on to the DCF CIO for their review and signature. Once the CIO has signed the DSA, the hardcopy should go to the IT Data Agreement Coordinator to be scanned into electronic format and entered into the OITS EDM System. Data specifications inventory shall include storage locations, exchange time, and record details. Upon completion the entire DCFTracker packet including the signed hardcopy should go back the DCF Agreement Coordinator.

g. DCFTracker Close Out. The respective DCF program office Agreement Coordinator will be responsible for coordinating the closing the DCFTracker Issue Number.

h. Existing DSAs. Changes, renewals, modifications, or other alterations to existing DCF Data Sharing Agreements will also be sent through DCFTracker as part of the DCF internal review process and are also required to go through the same review process.

7. Procedures for DCF Memorandums of Agreement, Memorandums of Understanding, and other DCF Data Sharing Initiative Agreements.

a. For any agreement templates other than the Data Sharing Agreement template (form CF 122, available in the DCF Forms), for example, Memorandums of Agreement, Memorandums of Understanding, and any other type of DCF data sharing initiative agreement, DCF employees are expected to follow the same review process:

(1) Enter Draft into DCFTracker;

(2) Complete the Described Draft Review Phase;

(3) Complete the Entire Described Review for Signature Phase; and,

(4) Complete the DCFTracker Close Out, including ensuring the OITS Data Agreement Coordinator receives a copy of the signed DSA for entry into the OITS EDM System.

b. Changes, renewals, modifications, or other alterations to existing DCF data sharing initiative agreements will also be entered into and sent through DCFTracker as part of their DCF internal review process as set forth in this operating procedure.
8. Procedures for Internal OITS Maintenance and Review. OITS is responsible for documenting in a Standard Operating Procedure (SOP) any OITS processes and procedures associated with OITS review and maintenance of signed DCF Data Sharing Agreements within the OITS EDM System.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

JULIE MADDEN
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Revised and updated to comply with Chapter 60GG-2, Florida Administrative Code.