TITLE	POLICY NUMBER	
Data Sharing Agreements	DCS 07-19	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
Audit Management Services	09/15/22	1

I. POLICY STATEMENT

This policy governs the development and maintenance of Data Sharing Agreements (DSAs) whenever data is exchanged between the Department of Child Safety (DCS) and external entities. The purpose of this policy is to establish guidelines and processes that protect the integrity, security, and confidentiality of data in accordance with DCS mission, vision, and values. Any data shared by the Department, whether received from or disclosed to another entity, will be governed by a comprehensive DSA, and an attendant Memorandum of Understanding (MOU) or other applicable agreement such as an Interconnection Security Agreement (ISA) or Intergovernmental Agreement (IGA) that precisely defines the details and expectations of the data sharing project. If DCS receives data from an external entity, it is incumbent on that entity to execute the MOU, ISA, or IGA. This policy shall not be construed to supersede any federal and state statutes or rules related to data governance.

II. APPLICABILITY

This policy shall apply when an external entity requests that data stored in a DCS system of record, such as the child welfare information system known as Guardian, to be shared. This policy also applies when data that emanates from an external entity is shared with DCS. If DCS is requesting data from an external entity, DCS will abide by the external entity's templates and processes.

III. AUTHORITY

A.A.C. R21-1-107	Release of DCS Information for a Research or Evaluation Project

A.R.S. § 8-807	DCS information; public record; use; confidentiality; violation; classification; definition
HIPAA 45 CFR § 160.103	Health Insurance Portability and Accountability Act
Section 106(b)(2)(B)(viii)	Child Abuse Prevention and Treatment Act

IV. DEFINITIONS

Breach: All known incidents that result in the unauthorized access, use, or disclosure of data protected by federal or state laws.

Business Intelligence: A technology-driven process for analyzing data and delivering actionable information that help leaders and workers make informed decisions.

Business Owners: DCS leaders identified as the owner of a functional area within the Department.

Data Sharing Agreement (DSA): A formal document of agreement between two entities that specifies the conditions under which data is shared. It is signed by appropriate authority from each party involved and includes, but is not limited to, the criteria for access to data, how it may be used, conditions of data use, retention of data periods, and the duration and effective date of the agreement.

Data Sharing Agreement Amendment: A document used to extend, modify or terminate a Data Sharing Agreement.

Department or DCS: The Arizona Department of Child Safety.

External Entity/Requestor: Any person, entity, or organization (e.g., government agencies, academic institutions, community partners, child-serving organizations, etc.) that requests DCS data and is a party to an approved Data Sharing Agreement.

Guardian: The comprehensive child welfare information system (CCWIS) employed by DCS that comprises extensive data and technological solutions to enhance child safety.

Interconnection Security Agreement (ISA): A contract that specifies information security requirements for system interconnections, including the security requirements expected for the impact level of the data being shared for all participating systems.

Intergovernmental Agreement (IGA): A type of contract agreement where two or more public agencies may contract for services or jointly exercise any powers common to the contracting parties and may enter into an agreement together for joint or cooperative action, as long as each agency has been authorized by their legislative or other governing body.

Memorandum of Understanding (MOU): A written document that outlines the terms and conditions of how data will be transferred and privacy rights associated with the transfer of confidential or protected data.

Notice: A notification of a fact, claim, demand, or proceeding. Notice may also encompass routine, workaday communications between DCS and the external entity.

Personally Identifiable Information (PII): Any information about an individual maintained by an 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.

Protected Health Information (PHI): Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium (HIPAA 45 CFR § 160.103).

Protected Individual: A living person who is the subject of a DCS investigation and others whose personal information is confidential under A.R.S. § 8-807.

Recipient: Any person, entity, or organization that is a party to an approved Data Sharing Agreement that receives data sets for authorized purposes.

V. POLICY

A. Data Sharing Standards

1. General Provisions

a. Data sharing will be governed, construed, and enforced in accordance with the laws of the state of Arizona.

b. Notices and communications between the parties will be relayed in writing by:

i. personal delivery;

ii. a nationally recognized, next-day courier service;

iii. first class registered or certified mail, postage prepaid;

iv. electronic submission to an address that one party has notified the other to be that party's electronic address.

Notices will be effective upon the other part's receipt of it, or, if physically mailed, upon the other party's receipt of it, or upon the fifth business day after it was mailed, whichever is earlier.

2. Data Sharing Agreements and Memoranda of Understanding

Data maintained by DCS shall only be shared with external entities that enter into a written DSA with DCS, and an accompanying Memorandum of Understanding (MOU), or Interconnection Security Agreement (ISA), or Intergovernmental Agreement (IGA).

a. The DSA shall convey the agreement details, including the purpose of the exchange, the responsibilities of the data recipient, the cadence of sharing, confidentiality requirements, permitted disclosures, and other provisions designed to ensure that data is shared safely, securely, and ethically. Any disclosure of data contrary to the DSA is unauthorized and is subject to penalties identified in law. Neither party to a DSA may assign to a third party any of their rights or obligations without the other party's written consent.

b. The MOU will document the business needs and justifications associated with the project.

3. Safeguarding Personally Identifiable Information and Protected Health Information

a. Whenever possible, DCS shall share anonymized, aggregated data

that excludes any information that could be used to identify any protected individuals, including children, family members, other persons mentioned in the case record, or Department staff. Unless written consent is obtained from the parent(s) and/or a child 18 years of age, Department information will be released to requestors only in forms that do not allow identification of the aforementioned individuals.

b. If Personally Identifiable Information (PII) or Protected Health Information (PHI) is shared by DCS, the requestor shall not use, disclose, or share it in a manner prohibited under federal or state law or regulation.

c. Recipients of data shall not attempt to identify any persons whose information is contained in the data or attempt to contact those persons.

4. Data Sovereignty and Accuracy

DCS makes no assurance of the accuracy and completeness of the data it shares with external entities; some data fields may contain incorrect or incomplete data.

5. Duration of Data Sharing Agreement

DSAs shall remain effective for one (1) year, unless otherwise stipulated. If the data recipient wishes to extend the term identified in the DSA, a written request for an extension must be submitted to the Privacy Officer. Extensions must be requested no less than sixty (60) days prior to the termination of the DSA. If approved, the DSA will be amended.

6. Termination of Data Sharing Agreement

Either party may terminate the DSA by delivering a termination notice to the other party if:

a. the other party fails to perform, has made or makes any inaccuracy in, or otherwise materially breaches any of its obligations, covenants, or representation;

b. the failure, inaccuracy, or breach continues for a period of five (5) business days after the injured party delivers notice to the breaching party reasonably detailing the breach.

7. Return or Destruction of Data and Property

Upon expiration or termination of the DSA, the recipient will immediately:

a. return all the data (including confidential information) provided by DCS that the recipient still maintains in any form;

b. securely destroy all copies of the data and other related property in its possession;

c. deliver to DCS a certificate of destruction confirming compliance with this destruction obligation (if required by DCS);

If it is not feasible to return or securely destroy the data, the recipient will provide written notification of the conditions that make return or destruction unfeasible within ten (10) business days, in which case the recipient will continue to protect all data that it retains.

B. Data Recipient Responsibilities

Recipients will abide by all terms and conditions outlined in DSA and MOU, including:

1. complying with all applicable laws and regulations relating to the collection, storage, access, use, or disclosure of DCS data;

2. restricting access to the data to authorized users only;

3. disclosing the data only if necessary and in furtherance of the purpose of the DSA/MOU and in compliance with applicable federal and state law. The recipient shall:

a. notify the Privacy Officer in writing within 24 hours if the recipient is required by law to disclose any of the data;

b. seek the prior consent of DCS prior to disclosing any of the data;

c. only disclose the data to DCS directors, officers, or employees who need to know, are aware of the obligations contained in the DSA, and agree to abide by its provisions.

4. protecting the confidentiality of data by preventing unauthorized access, use, or modification of the information by:

a. establishing and maintaining safeguards against the misuse, damage, or disclosure of the DCS data in its possession;

b. maintaining adequate physical controls, access, and password protections for any system (whether paper or digital) in which the data is stored;

c. ensuring the data is not stored on a mobile device;

d. transmitting the data only if it is encrypted;

e. taking all measures necessary or required by law to prevent any use or disclosure of the data other than as allowed by the DSA.

5. ensuring that any agents, or subcontractors, to whom data is provided agree to the same restrictions and conditions that apply to the recipient.

6. refraining from decompiling, modifying, reverse engineering, or creating derivative works from the data;

7. making an immediate verbal report to the Privacy Officer when any unauthorized use or disclosure of data occurs, following up with a written notification within 24 hours, and cooperating with DCS regarding any remediation the Department believes is necessary. The written notification will include a description of the incident, what data was involved, the person or organization that received it, and what actions have been taken to mitigate potential negative effects;

8. securing the permission of DCS, while the DSA is active, prior to publishing or presenting any findings or conclusions gleaned from the data; after the completion of the term of the DSA, no publication or any

other release of DCS information will be permitted without the express written permission of DCS. Exceptions apply when publications are related to research findings.

C. Dispute Resolution

The responsibility for resolving data access disputes between DCS and an external entity will include the Privacy Officer and the Business Intelligence Team.

D. Post-DSA Auditing

During the term of the DSA, and for six (6) years thereafter following its expiration, DCS has the right to access the recipient's records and place of business for the purpose of auditing and evaluating compliance with the DSA and applicable laws and regulations. DCS will provide the recipient written notice at least five (5) business days prior to its intention to commence an audit.

VI. PROCEDURES

A. Data Sharing Requests

1. When an external entity approaches a DCS business owner to request data, both parties will discuss the request and determine the benefits of potential data sharing. The business owner will ask the requestor to submit the request in writing and forward it to the Privacy Officer.

    a. When a request involving the exportation of data from DCS to an external entity is received, the Privacy Officer will send the requestor a link to the DSA and ask them to complete it.

    b. If there is a need to import data to DCS from a requestor, the Privacy Officer will discuss with the requestor the need for the data, and will request the external entity's DSA template for completion and signatures. If no data will be imported from the requestor, no DSA is needed.

    c. If the requested data is to be used for research purposes, the Privacy Officer will refer the requestor to the Research Review

Committee by sending a link to the *Research Review Committee (DCS-1561)* form to describe their research project. After this referral, no further action is needed; the Research Review Committee will commence their process to review the request in compliance with the *Research Review Requests* (*DCS 14-02*) policy.

B. Data Sharing Request Review

1. The Privacy Officer will ascertain if there are any laws or policies that prohibit the data sharing sought by the requestor. If there are none, the process will proceed to the next step.

2. The Privacy Officer, Business Owner, and Business Intelligence Team will review the draft DSA submitted by the requestor to ensure that the information is correct, current, and in alignment with the business need, which will be outlined in an MOU. Business Intelligence determines if the data is available and if the requestor's preferred method of data transmission can be accommodated, and the Interface Administrator and the Business Owner will validate the data fields that are being requested.

3. If the DSA requires more information, the Privacy Officer will identify the missing or incomplete information and send it back to the requestor for revision.

C. Memorandum of Understanding

In conjunction with the Data Sharing request and review process cited above, an MOU or other applicable agreement may be created before a DSA can be fully executed. The MOU created by DCS Procurement and Contracts, summarizes the details of the data sharing request. It meticulously describes the specific mechanics of data sharing between the requestor and DCS.

D. Data Sharing Agreement Approval

1. If the DSA is complete and approved by all reviewers, the Privacy Officer will create an official DSA number and route it for DCS signatures.

2. After DCS signatures are obtained, the DSA is forwarded to the requestor for signatures. The requestor sends the signed DSA back to the Privacy

Officer.

3. The Privacy Officer informs the Business Intelligence team that the signed DSA has been returned from the requestor, and work may commence on fulfilling the request.

4. The Privacy Officer will send a copy of the fully executed DSA to the Contracts Unit to be merged with any corresponding overarching MOU.

E. Data Sharing Agreement Contents

The fully executed DSA will contain the following fields:

1. DCS DSA Number - the official contract number provided by the Privacy Officer.

2. DCS MOU Number - provided by DCS Contracts, the number of the MOU that describes the business needs for which the data will be used.

3. Agreement Date – the start date of the DSA.

4. The name, address, and abbreviation (if applicable) of the external requestor.

5. Description of purpose - a high-level summary of how the data will be used.

6. Description of Data – the specific data (e.g., name, date of birth, etc.) that will be shared.

7. Attachment – the name that accompanies the DSA and contains data fields and descriptions.

8. Frequency of Sharing – the rate of recurrence that data will be shared (e.g., weekly, monthly, quarterly).

9. Method of Data Sharing – a simple description of how the data will be shared (e.g., data exchange using an Application Programming Interface, or an encrypted flat file).

10. The name, title, email address, and phone number of the DCS resource who understands the business need for the data.

11. The name, title, email address, and phone number of the external requesting resource who understands the business need for the data.

12. The name, title, and signature of the DCS resource who has the signature authority to execute the DSA.

13. The name, title, and signature of the external requesting resource who has the signature authority to execute the DSA.

F. Amendments

A DSA must be amended or replaced if changes to the terms of the agreement are agreed upon by DCS and the requestor. An amendment shall be processed using the *Data Sharing Agreement Amendment* (DCS-1182A) form and must be signed by DCS and the requestor. The form may be used to extend, modify, or terminate a DSA.

G. Terms of Length

DSAs are in effect for a period of one (1) year, unless otherwise specified. If data access is no longer needed during the standard one-year period, it may be terminated upon mutual agreement of the parties.

VII. FORMS INDEX

Data Sharing Agreement

Data Sharing Agreement Amendment (DCS-1182A)