TITLE	POLICY NUMBER	
Transporting Confidential Records and Information	DCS 02-07	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
Business Operations	April 13, 2018	

I. POLICY STATEMENT

It is the policy of the Department of Child Safety (DCS) to ensure the appropriate and secure transportation of confidential records and information. Confidential records and information shall not be transported outside an employee's work area unless necessary to complete DCS assigned work duties. Any confidential records or information that must be transported outside of the work area shall be secured at all times.

II. APPLICABILITY

This policy applies to all DCS employees.

III. AUTHORITY

A.R.S. § 8-453	Powers and duties
A.R.S. § 8-807	DCS information; public record; use; confidentiality; violation; classification; definition

IV. DEFINITIONS

Confidential information: Non-public information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or damage the person or entity's financial standing, employability, privacy or reputation. DCS is bound by law or contract to protect some

types of confidential information, and in other instances requires protection of confidential information beyond legal or contractual requirements as an additional safeguard.

Confidential data: Paper or electronic information which, if improperly used, released, or tampered with, could cause serious loss of personal privacy, injury to the State of Arizona, loss of competitive advantage, loss of confidence in a government program, financial loss, or affect legal action and cause damage to partnerships, relationships, and reputations. Includes Federal Tax Information (FTI), Protected Healthcare Information (PHI), and Personally Identifiable Information (PII) or any other information that is statutorily confidential under state or federal law.

Employee: All DCS full-time, part-time, intermittent, and temporary employees; all students, interns, and volunteers.

Federal Tax Information (FTI): Federal tax return and return information received by specific state agencies from the Internal Revenue Service (IRS) as defined and regulated by IRS Publication 1075. Federal law 26 U.S.C. § 6103 also specifies the regulations regarding maintaining confidentiality of FTI.

Personally Identifiable Information (PII): Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Protected Healthcare Information (PHI): Any health-related information that can be tied to an individual is considered protected health information.

V. POLICY

DCS employees shall not misuse confidential records and information.

A. Confidential records and information shall not be transported outside the office unless necessary to complete DCS-assigned job tasks.

B. All employees with job duties that require them to handle confidential records and information are required to safeguard such information and only use it or disclose it as expressly authorized or specifically required in the course of performing their specific job duties.

C. Misuse of confidential records and information can be intentional (acts and/or

omissions) or a product of negligence or carelessness. Misuse includes but is not limited to:

1. accessing information not directly germane or relevant to the employee's specifically assigned tasks;

2. disclosing, discussing, and/or providing confidential information to any individual not authorized to view or access that data, including but not limited to third parties, volunteers, vendors, and other DCS employees;

3. reckless, careless, negligent, or improper handling, storage, or disposal of confidential data, including electronically stored and/or transmitted data, printed documents, and reports containing confidential information;

4. deleting or altering information without authorization;

5. generating and/or disseminating false or misleading information;

6. using information viewed or retrieved from DCS systems for personal or unauthorized/unlawful use;

7. sharing information broadly across social media or other forms of publically accessed networks.

D. Employees are expected to:

1. identify confidential information and materials by maintaining annual certification on Security Awareness Training;

2. proactively seek information regarding and comply with any restrictions on the use, administration, processing, storage or transfer of the confidential information in any physical or electronic form; see the following policies for more information:

   a. Data Classification (DCS 05-03);

   b. Media Protection (DCS 05-10);

   c. Acceptable Use (DCS 05-13).

3. learn about and comply with any procedures regarding the appropriate handling of such information and materials by completing any and all required State/DCS sponsored required training.

4. understand their responsibilities related to information security.

E. Employees who have access to confidential information are expected to know and understand associated security requirements, and to take measures to protect the information, regardless of the data storage medium being used. This includes printed media (forms, work papers, reports, microfilm, microfiche, books), computers, data/voice networks, physical storage environments (offices, filing cabinets, drawers), or magnetic and optical storage media (hard drives, diskettes, tapes, CDs, flash drives). Computer display screens should be positioned so that only authorized users can view confidential information, and confidential information should be discarded in a way that will preserve confidentiality (e.g., in a shred box, not in a trash can or recycling bin).

F. Employees must report any violation of these guidelines immediately to their supervisor, manager, or administrator. An Unusual Incident Report shall be completed to document the violation; see the Unusual Incident Reporting Policy (DCS 02-12) for more information.

G. Employee misuse of confidential information and/or the systems in which the information is stored is a serious breach of job responsibilities and may result in discipline up to and including termination of employment.

1. When possible, employees will make copies of original documents and only take copies out of the office. If originals are needed, the employee will be responsible for tracking what originals have been removed from the office.

2. Employees will only take what confidential information they need out of the office and shall minimize the time that confidential data is out of the office. Employees shall not take confidential data out of the office sooner than necessary and shall return it as soon as practical to the office.

3. Printing confidential data from a publically accessed and managed printer is prohibited.

4. Confidential information and technological equipment shall never be stored in vehicles overnight. All such information and equipment shall be removed from vehicles prior to the end of the workday.

H. All containers housing confidential information must be marked as such before the records leaving the office. Any boxes, files, or other physical information must clearly be marked using a label or other device to show that the contents are

confidential.

I. If it is necessary to remove case files/records and keep them out of the office for more than one business day, a notice must be sent to a supervisor that lists the name of the records that have been removed or the case ID for each case file.

VI. PROCEDURES

A. Transporting Records during Business Hours

If required to be transported outside the office, any confidential record or information must be kept secure whenever not in use. Acceptable methods of protecting confidential records and information outside the office include:

1. keeping confidential records and equipment in the physical proximity and under the close supervision of the employee;

2. keeping confidential records and equipment in a lock box, locked filing cabinet, or locked case;

3. locking confidential records and equipment in a car trunk. Confidential records and equipment should only be stored in vehicles when there is no other secure option available. Such information or equipment should only be locked in a vehicle trunk or other secure area during the workday;

4. hiding confidential records and equipment from plain sight.

B. Transporting Records Overnight

When keeping confidential records or information out of the office for one or more business day, the following steps must be taken to safeguard the information:

1. A notice should be sent to the employee's supervisor with a list of what records or associated Case IDs for information is being stored with the employee outside of the office with an estimated return date/time.

2. Confidential records and information should be kept inside the same dwelling as the responsible employee. No records (physical or electronic) should be left in a vehicle overnight.

3. If roommates, family, or other unauthorized viewers could have access to

the confidential records or information, the employee must ensure that the records are stored under lock and key. Alternatively, the employee may store the records within a container that is clearly labeled as confidential, if a lockable container is not available.

4. Employees must remain aware of the whereabouts of confidential records and information for the entire duration that the records are out of the office.

5. Upon return to the office, the employee is responsible for returning the records to their original storage location and notifying their supervisor that the records have been returned.

VII. FORMS INDEX

Unusual Incident Report (DCS-1125A)