



TITLE	POLICY NUMBER	
Data Storage	DCS 05-23	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	July 2, 2018	2

I. POLICY STATEMENT

The purpose of this policy is to establish the policy for storing or saving personally identifiable information (PII), confidential data, and documentation on the Department of Child Safety (DCS) equipment.

II. APPLICABILITY

This policy applies to all DCS information systems, processes, operations and personnel to include all employees, contractors, interns, volunteers, external partners and their respective programs and operations.

III. AUTHORITY

[HIPAA Administrative Simplification, Security and Privacy, 45 CFR Part 164, March 2013.](#)

[IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Revision 9-2016.](#)

[NIST 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.](#)

IV. DEFINITIONS

Confidential data: Data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements.

Department or DCS: The Arizona Department of Child Safety.

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.

V. POLICY

A. Proper and Security and Storage of Personally Identifiable Information

Documentation and confidential data, as described in the Data Classification Policy ([DCS 05-03](#)), is the responsibility of all DCS employees. DCS has defined approved and unapproved storage of PII, documentation and confidential data as follows:

1. Approved Storage Locations
 - a. DCS OneDrive;
 - b. shared drive;
 - c. SharePoint;
 - d. DCS email;
 - e. OnBase Storage.
2. Unapproved Storage Locations:
 - a. thumb drive or USB drive;
 - b. external hard drive;
 - c. non-DCS email;
 - d. personal or home computer or laptop;

- e. personal cloud storage accounts;
- f. personal mobile devices:
 - i. mobile phone;
 - ii. tablet.