

[Back to Top ^](#)



Print Section

Print Entire Policy

[Confidentiality](#) > [Responses and Protections](#) > [Confidentiality of Mobile Workers](#)

Confidentiality Protocols for Mobile Workers, Teleworkers, and Portable Devices

0500-507.10 | Revision Date: 07/01/14

Overview

This policy reviews the process that ensures the confidentiality of case record information and supporting documents when teleworking and/or using mobile or portable devices.

TABLE OF CONTENTS

Policy

- [Teleworkers and/or Mobile Workers Standards](#)
- [Confidentiality Protocols](#)

Approvals

Helpful Links

- [Referenced Policy Guides](#)
- [Statutes](#)

Version Summary

This policy guide was updated from the 12/05/11 version, as part of the Policy Redesign, in accordance with the DCFS Strategic Plan.

POLICY

Telework, or participation in the Mobile Worker program, requires that staff take steps to ensure the confidentiality of departmental case record/information. Upon completing a specific case task, staff must properly dispose of materials that are not going to be part of the case record.

Teleworker and/or Mobile Worker Standards

The following standards apply to all teleworkers and/or Mobile Workers:

- Teleworking and/or Mobile Worker Program are entirely voluntary and may be terminated by the employee or the Department at any time.
- The duties, obligations, responsibilities and conditions of a teleworker's and/or mobile worker employment with the Department are unchanged.
- Work hours, overtime compensation and vacation schedule will conform to the federal Fair Labor Standards Act (FLSA), County Code and to MOU provisions.
- Employees remain obligated to comply with all County rules, policies, practices and instructions.
- Requests to work overtime, use sick leave, vacation or other leave must first be approved by the employee's supervisor in the same manner as when working in the regular office.
- If the teleworker and/or mobile worker is sick while working at home, the teleworker/mobile worker is required to report the hours worked, and must use sick leave or other accrued time to cover the hours not worked.

Confidentiality Protocols

- The use of equipment, software, and data supplies, when provided by the Department for use at the offsite work location, is limited to authorized persons and for purposes relating to County business.
- Critical confidential documents such as court reports and other sensitive material must not be e-mailed or faxed from a teleworking location to regional offices or other locations.
- Do not allow anyone to access case records and/or case materials while working at a teleworking location or traveling between the office and teleworking location.
- Conduct all phone calls related to casework in private.
- Do not verbally disclose confidential case information to any unauthorized person, e.g., family members, friends, etc.
- Always lock case records in the trunk of your car when transporting them and never leave case records unattended. Transport case records in brief cases, carrying bags, or boxes so that confidential information is not exposed.
- Do not store case records on the hard drive of a personal computer or leave computer disks that contain case record information at a teleworking location.
- Original client files shall not be stored at alternative work locations. However, copies of need documents may be stored at an alternative work location.
- Return all case records and/or case materials to the regional office on the first business day you return. Do not leave case records and/or case materials in your teleworking location, even if the tasks are not completed or documents are to be shredded.
- Upon return to the office, ensure that all partially completed forms, case notes, worksheets, extra copies of photocopies which contain any person and/or case-specific information (e.g., case name, case number, etc.) that are no longer needed, are shredded.

- If shredding machines are not directly available, place the material in a collection bin expressly designated for material that is to be shredded. Do not place materials containing person and/or case-specific information in recycling bin/boxes or trash baskets until it has been shredded.
- Upon return to the office, delete from any disks, tablets, laptops, flash drives, and/or hard drives all partially completed forms, case notes, worksheets, etc., that are not going to be part of the case record and are no longer needed.
- Immediately report any lost, stolen or damaged records to the SCSW and/or ARA.

[Back to Policy](#)

APPROVALS

None

HELPFUL LINKS

Referenced Policy Guides

[Information Technology Alert 11-01](#), Remote Access/MYPC/RSA Secured Token Management Directive 11-02, Use of Department Portable Computer/Electronic Devices

Statutes

[Welfare and Institutions Code 827](#) – Provides regulations pertaining to juvenile case file inspection, confidentiality, release, probation reports; destruction of records; and liability.