

MANAGEMENT DIRECTIVE

USE OF DEPARTMENT INFORMATION TECHNOLOGY RESOURCES

Management Directive # 08-01

Date Issued: 10/ 30 /15

- New Policy Release
- Revision of Existing Management Directive MD # 08-01 Use of Department Information Technology Resources, dated 10/14/08

Revision Made: This policy was updated to add additional personal and storage devices that are prohibited to use for County/Department data unless permission is granted by the Bureau of Information Services.

Cancels: None

DEPARTMENTAL VALUES

The Department continues to focus on the three priority outcomes. We have identified improved safety for children, improved timelines to permanency. Timely permanence is achieved, with the first permanency option being reunification, followed by adoption with a relative and legal guardianship with a relative followed by adoption with an unrelated caregiver and legal guardianship with an unrelated caregiver.

APPLICABLE TO

This directive applies to all Department staff (County employees, contractors, sub-contractors, volunteers and other governmental and private agency staff) who make use of County and/or Department Information Technology Resources.

OPERATIONAL IMPACT

This directive also contains an "Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data" to be signed by all staff with access to computers or computer-generated data at the time of employment and annual Performance Evaluation review.

The intent of this policy is to ensure that all employees are aware of their role and responsibilities in the use and protection of the County's/Department's Information Technology Resources.

DEFINITIONS

A. Computer Data

All data entered and maintained in any computer system, and all programs and documentation constituting those systems, whether developed by or for the County or licensed to the County. Data may be in any form: in storage media; in computer memory; in computer printouts; or presented on a display device.

B. Availability of Data

The availability of data for its intended use, when and where needed.

C. Confidentiality of Data

The sensitivity of computer data or information that could cause harm from its unauthorized disclosure.

D. Integrity of Data

The accuracy (no errors or unauthorized changes), completeness (nothing added or deleted), and currency (all known changes are present) of records.

E. Data Security

The protection and preservation of confidentiality, integrity, and availability of Department information technology resources.

F. Computer Virus

A software program that may be loaded onto a computer, usually without the knowledge of the user, and runs against the user's wishes. Viruses can replicate themselves. All computer viruses are man-made. A computer virus can use all available computer memory and bring the system to a halt.

G. Department Information Technology Resources

Department Information Technology Resources include but are not limited to the following:

- Computers and any electronic device which stores and/or process County data (for example: desktops, laptops, midrange, mainframes, PDAs, County wired or wireless networks, digital cameras, copiers, IP phones, faxes, pagers, related peripherals, etc.)

- Portable Media on or off Department premises
- Network connections (wired and wireless) and infrastructure, including jacks, wiring, switches, patch panels, hubs, routers, etc.
- Data contained in Department systems (databases, emails, documents, repositories, web pages, etc.)
- Department purchased, licensed, or developed software.

H. Portable Storage Media

Portable storage media include, without limitation, the following:

- Diskettes
- Tapes
- CDs / DVDs
- Zip disks
- Flash memory/drives
- USB drives

I. Network

A system that links computers together and allows for exchange of information, applications and sharing resources such as printers.

J. Passwords/User IDs

A group of characters by which a user is uniquely identified when accessing computer systems or networks. Passwords may be different for each data system that an employee has access [e.g., Child Welfare Services/Case Management System (CWS/CMS), Welfare Case Management Information System (WCNIS), MEDS, AWINS, DMV, Internet, Intranet, etc.] Passwords are used to limit access to computer systems to authorized persons. There are separate data security registration forms for each computer system or group of computer systems.

K. Peripherals

Any device, such as an external diskette drive, printer, or terminal that is used for input or output operations with the computer. Each device is part of a computer system and operates under the control of that computer.

L. Authorized Software

Any software purchased, licensed and installed by the Department on Departmental computer systems intended for the business use of staff.

M. Unauthorized Software

Any software not owned, licensed or installed by the Department on Departmental computer systems.

N. Software License Agreement

The contract or agreement under which software is purchased or rented from the manufacturer. The Software License Agreement limits the way(s) in which the software may be used, usually including limits to concurrent use on more than one machine and/or by more than one user at a time.

POLICY

- A. Department Information Technology Resources are to be used for County business purposes only.
- B. Use of Department Information Technology Resources is subject to audit and periodic unannounced review by authorized individuals as directed by County and/or Department management. The County and the Department of Children and Family Services reserve the right to override any individual password and access all data contained on those resources for any business purpose.
- C. Department employees shall not intentionally or through negligence damage, interfere with the operation of, or prevent authorized access to County information technology resources. It is every user's duty to use the County's resources responsibly, professionally, ethically, and lawfully.
- D. Users expressly waive any right of privacy in anything they create, store, send or receive through County technology resources, with the exception of legally protected information.

This is required for the Department to meet its obligations to the public by safeguarding confidential information against potential misuse, abuse or loss.

- E. Unless expressly authorized by Department management or policy; sending, disclosing, or otherwise disseminating confidential data, protected information, or other confidential information of the County is strictly prohibited. This includes information that is protected under privacy legislation.

- F. Department employees are not to access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by County and/or Department management.
- G. Department employees are not to intentionally introduce any computer virus, worms, or malicious code into any County or Department computer, network, system or data.
- H. Department employees are not to access or send any offensive materials, e.g., pornographic, racial, harmful or insensitive text or images, over Department owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of assigned job duties, e.g., law enforcement. Employees are to report any offensive materials observed by the employee or sent to the employee on Department systems to their immediate supervisor
- I. The Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. Use of the County provided Internet services is for approved County business purposes only, e.g., as a research tool or for electronic communication. The County's Internet services, although filtered, may expose the employee to offensive materials. The County and Department are to be held blameless should any employee be inadvertently exposed to such offensive materials. **Employee Internet activity is logged and is subject to unannounced audit and review by authorized individuals.**
- J. Electronic mail (e-mail), and data, in either electronic or other forms are subject to unannounced audit and review by authorized individuals. Employees are to maintain and use proper business etiquette when communicating over e-mail systems. Please review Management Directive 08-02, Use of Department Email.
- K. Department employees are not to subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. Employees are not to share computer identification codes (log-in ID, computer access codes, account codes, ID's etc.) or passwords.
- L. At the time of logging onto the Department computer and network, each user is presented with a log on banner which summarizes many points of this Management Directive. The employee acknowledges the content of the banner message by clicking the OK button to proceed with completing the log in process.
- M. It is the Department's policy **not** to provide computer hardware, software, and applications developed by the Department for use on personal home computers.
- N. It is the Department's policy that each employee and their immediate supervisor shall sign and date the "Agreement For Acceptable Use of DCFS' Information Technology Resources" form after reading this policy material.

This form is to be signed upon receipt and reading of this Directive and annually at the time of Performance Evaluation review. This is to ensure that all employees understand the importance of protecting the confidentiality of the County's and Department's data and the guidelines outlined herein.

- O. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contactors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

PROCEDURES

A. PHYSICAL SECURITY

Unauthorized access to any County and/or Department information technology resources, including the computer system, network, software application programs, data files, and restricted work areas is prohibited.

Formal measures must be taken to protect all information technology resources from theft. All computers must be locked down. Requests for physical lock-down of computers should be directed to the Bureau of Information Services. Laptop computers, printers and easily concealed items such as printer output, portable media and manuals should be secured when not in use.

B. USE OF PERSONAL INFORMATION TECHNOLOGY RESOURCES

Use of personal (not County/Department owned) information technology resources to access and/or store County/Department data is strictly prohibited unless permission is granted by the Bureau of Information Services. This includes but is not limited to personal storage devices, such as; third party email systems and storage servers, USB Drives, Flash Drives, Cloud based storage, external portable data storage or hard drives, CDs, DVDs, Laptops and Personal Digital Assistants (e.g. hand held smart device, Smart Phones, electronic data storage media, etc.)

Personal software (software purchased or downloaded from the Internet by an employee) must not be installed on desktop or portable computers without prior approval from the Bureau of Information Services.

C. SOFTWARE COPYRIGHT PROTECTION

NOTE: *Unauthorized copying of packaged software is a violation of software licensing agreements and/or federal copyright laws and can result in legal action by the software manufacturer against the employee, the County, and/or the Department.*

Commercial software may not be duplicated or used on a computer system other than the unit for which it was originally installed.

Questions regarding manufacturer's copying policies and licensing agreements are to be directed to the Bureau of Information Services.

All materials, documents, written designs, plans, reports, diagrams, training aids, documentation, systems, applications, software, source codes, object codes, templates, tapes, diskettes, models, tools of all types, etc, developed or acquired for Departmental use are the sole property of the County and shall not be removed, modified or duplicated without the permission of the Bureau of Information Services.

Employees involved in systems or applications development shall disclose and make available to Department management all items mentioned above and any other tangible incidents of their work, since the County owns and is entitled to benefit from all work developed or conceived by an employee while in the employment of the County.

D. DATA INTEGRITY

All employees are responsible for maintaining the integrity of Departmental data. They shall not knowingly or through negligence cause Departmental data to be modified or corrupted in any way that compromises its accuracy or prevent authorized access to it.

E. DATA SECURITY

All diskettes and backup tapes are to be clearly marked with the user's name and diskette or tape contents. Most of the techniques used to protect data are simple, common sense methods. Others are more technical. Below are several methods available for protecting the confidentiality of data:

- Maintain a high level of awareness of security and its importance;
- Restrict public access to areas through use of signs and/or locks;
- Lock your office, desk, filing cabinet, or terminal cabinet;
- Control the disposal of printer output through shredding or other approved methods;
- Control the distribution of data through logs and/or signed transmittals; and
- **Do not leave applications open or running on the computer screen when you are away from your desk.** Close the application or software or Log-off (if necessary) even if you feel you will be away from the screen for five minutes or

less. This also includes word processing documents, Electronic Mail, and inquiry screens for CWS/CMS, WCMIS and APPS.

E. RELOCATION OF COMPUTER EQUIPMENT

The Bureau of Information Services is responsible for relocating all computer equipment within the Department. County-owned or leased desktop computer systems are not to be relocated within or removed from the premises without formal approval of the Bureau of Information Services.

F. PORTABLE STORAGE MEDIA

Only Department provided portable storage media is to be used to access or store County or Department information.

G. RE-USE OF PORTABLE STORAGE MEDIA

Prior to re-use, portable media containing any information are to be erased by reformatting. This should be done to prevent any data contained on that media from being viewed or used by a new user of that media.

H. DISPOSAL OF PORTABLE MEDIA MATERIALS

Obsolete information contained on portable media is to be erased before disposal.

When reformatting of data is not feasible, all media containing confidential information, including printed information, should be destroyed in a secure manner that physically obliterates the information content of the media. The Bureau of Information Services can assist with disposal upon request.

I. DATA BACKUP AND RECOVERY

All backup and recovery procedures for the applications developed by the Department are to be followed in accordance with the instructions supplied by the Bureau of Information Services. These procedures are vital to a successful systems recovery in the event of a mechanical or unintentional loss of information.

J. PASSWORD PROTECTION

User IDs and Passwords are used to verify that system users are who they claim to be and protects the security of the system by controlling access.

Passwords/User IDs are normally used for computer system applications that involve processing secured or confidential information. Passwords/User IDs are not normally used in office automation-type applications such as word processing, spreadsheets, etc.

Passwords/User IDs can be issued for inquiry-only capability as well as data input. Your password is to be known only to you. **Do not write your Password/User ID down or give it to anyone other.** You are responsible for the use of your Password/User ID.

If you suspect or know that an unauthorized person knows your Password/User ID, immediately notify the Office Head.

APPROVAL LEVELS

Section	Level	Approval
A.-D	None	

LINKS

Board of Supervisor Policy Manual <http://countypolicy.co.la.ca.us>

RELATED POLICIES

Board of Supervisor Policy 3.040, General Records Retention and Protection of Records Containing Personal and Confidential Information

Board of Supervisor Policy 6.100, Information Technology Security Policy

Board of Supervisor Policy 6.101, Use of County Information Technology Resources

Board of Supervisor Policy 6.014, Use of Electronic Mail (e-mail) by County Employees

Management Directive 08-02, Use of Department Email

Management Directive 08-03, Use of Department Portable Computing Devices

FORM(S) REQUIRED/LOCATION

Hard Copy: **DCFS 5**, Agreement for Acceptable Use of DCFS Information Technology Resources

LA Kids: **DCFS 5**, Agreement for Acceptable Use of DCFS Information Technology Resources

This page intentionally blank.

County of Los Angeles
Department of Children and Family Services
AGREEMENT FOR ACCEPTABLE USE OF AND CONFIDENTIALITY OF COUNTY'S
INFORMATION TECHNOLOGY ASSETS, COMPUTERS, NETWORKS, SYSTEMS AND DATA

As a Los Angeles County employee, contractor, vendor or other authorized user of County/Department Information Technology (IT) resources including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT resources for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As a user of County's IT resources, I agree to the following:

1. Computer crimes: I am aware of California Penal Code 502(c) - Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.
2. Security access controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's. etc.) or passwords
3. Approved business purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.
4. Confidentiality: I will not access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.
5. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will install and maintain computer virus detection and eradication software on my personal computer, servers and other computing devices I am responsible for.
6. Offensive materials: I will not access or send any offensive materials, e.g., pornographic, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.
7. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services are unfiltered and in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.
8. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will maintain and use proper business etiquette when communicating over e-mail systems.
9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.
10. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, cancellation of contracts or both civil and criminal penalties.

County of Los Angeles
Department of Children and Family Services
CALIFORNIA PENAL CODE 502(c) -
“COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT”

Below is a section of the “Comprehensive Computer Data Access and Fraud Act” as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502.(c) Any person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission aids, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network

I understand that my activities, while using Department Information Technology Resources, may be logged, are a public record, and are subject to audit and review by authorized individuals as directed by Department and or County management, with or without prior notice

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

(Employee Signature)

(Date)

(Employee Name – Print)

(Employee Number)

(Supervisor’s Signature)

(Date)

(Supervisor’s Name – Print)

PREPARATION: Original and two copies
DISTRIBUTION: Original in employee’s Official Personnel Folder
One copy in employee’s Office Personnel Folder
One copy to employee