

# **INTERNET/E-MAIL USE POLICY SECTION 41200**

<b>TABLE OF CONTENTS</b>	<b>PAGE</b>
POLICY.....	1
PURPOSE.....	1
APPLICABILITY.....	1
AUTHORITY.....	1
DEFINITIONS.....	2
INTERNET/E-MAIL USE.....	4
UNACCEPTABLE INTERNET / E-MAIL USE.....	5
E-MAIL RETENTION.....	6
ROLES AND RESPONSIBILITIES.....	7
LIABILITY.....	8
CONTACT INFORMATION.....	8
EFFECTIVE DATE.....	8

---

## INTERNET/E-MAIL USE POLICY

---

### POLICY

The Department of Child Support Services (DCSS) employees are granted access to Internet and E-mail resources to facilitate communication and information sharing, to enhance productivity, and to access research and reference sources that assist in the performance of business-related duties. Internet access is a privilege and DCSS reserves the right to withhold Internet access. Employees who access the Internet and/or E-mail are to follow these guidelines, unless required to perform official DCSS business that would support an exception to this policy. Using these methods of communicating is basically no different than communicating on a state telephone or official letterhead. The same types of business principles apply.

The intentional use of state time and resources for personal advantage, gain, or profit is inconsistent, incompatible, and in conflict with the duties of DCSS employees providing authorized services to the department.

### PURPOSE

The purpose of this policy is to inform all DCSS staff and contractors of the proper use of DCSS' Internet and E-mail.

### APPLICABILITY

This policy is applicable to all employees of the Department and also by contractors and consultants (where applicable).

### AUTHORITY

Information Practices Act of 1977  
Privacy Act of 1974  
California Public Records Act  
DCSS Information Security Manual  
State Administrative Manual (SAM) 5300

**DEFINITIONS**

<b>TERM</b>	<b>DEFINITION</b>
Authentication	The process of identifying an individual usually based on a user name and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access (see authorized access) to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Authorized Access	<p>Authority to obtain information from DCSS applications and databases on a “need to know” basis, which means:</p> <ul style="list-style-type: none"> <li>A. The information will be used for the purpose of performing your official DCSS responsibilities and tasks.</li> <li>B. You are not getting information out of curiosity, or for personal reasons.</li> <li>C. You are not modifying accounts pertaining to you, your family members, friends, acquaintances, co-workers, etc.</li> <li>D. You are not viewing or modifying information on celebrities or other well-known persons unless doing so is part of your assigned job duties.</li> </ul>
Confidential Information	Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code, 6250-6265) or other applicable state or federal laws. Examples of confidential information might include name; address; social security number; financial information including income, deductions, credits, federal or state tax returns, debt collection information for child support, and/or court fees; personnel records; and criminal offender record information, including attorney-client information/work products.
Critical Application	An application that is so important to the agency that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs.
Data Files	Files that contain user-generated information, such as word processing documents, spreadsheets or a database.

TERM	DEFINITION
DCSS Systems	Any system or network which stores, forwards, accesses or processes data for any DCSS program or function. This includes systems owned by DCSS or their contractors, whether that contractor is private or public.
Employees	Individuals who have authority to access the DCSS network for business purposes. This includes DCSS management, staff, and contractors.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security.
Information Assets	<p>A. All categories of automated information, including (but not limited to) records, files, and data bases.</p> <p>B. Information technology facilities, equipment (including personal computer systems), and software owned or leased by state agencies.</p>
Information Integrity	The condition in which information or programs are preserved for their intended purpose; including the accuracy and completeness of information systems and the data maintained within those systems.
Information Security	The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure. This also includes ensuring that only authorized persons have access to the DCSS network infrastructure and information assets.
Information Technology (IT)	Computers, networks and associated supporting equipment, software and cabling.
Internet and E-Mail Resources	Includes staff, hardware, software, and supporting infrastructure.
Network Activity	Personal computers, data packets, electronic files, printed material electronic mail, data records, website communication, password sharing, software, hardware, modem or any other related items or functions performed using state property or conducting state business.
Personal Computer	A computer designed primarily for use by one employee.
Policy	A definite course of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions. A policy specifies what should be done. Policies are mandatory and require special approval when an employee requests taking a contrary course of action.

TERM	DEFINITION
Political Activity	Affairs pertaining to works or efforts associated with endorsing and/or promoting a political bias not supported by DCSS.
Right To Privacy	The Privacy Act, passed by Congress in 1974, establishes certain controls over what personal information is collected by the federal government and how it is used. The Act guarantees three primary rights: A. The right to see records about yourself, subject to the Privacy Act's exemptions. B. The right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete. C. The right to sue the government for violations of the statute including permitting others to see your records (i.e., personnel, medical, and other files involving personal information) unless specifically permitted by the Act.
Streaming	A technique for transferring data such that it can be processed as a steady and continuous stream.
System	A group of related computer hardware and/or software or applications, as well as any associated data that performs a certain function when working together.

### INTERNET/E-MAIL USE

DCSS employees are permitted to use the Internet and E-mail for the following reasons:

- A. Communication and information exchange directly relating to DCSS business, charter, and work tasks.
- B. Announcements of state laws, procedures, hearings, policies, services, or activities.
- C. Advisory, standards, research, analysis, and professional society or development activities related to DCSS job responsibilities.
- D. The union's representative shall be permitted incidental and minimal use of state electronic communication equipment ordinarily available during the regular course of business if (1) permitted by the employee's department for other non-business purposes; and (2) for representational purposes only; (3) provided it results in no additional cost to the state; and (4) provided it does not interfere with the operations of the state.

- E. Incidental personal use, such as looking up medical appointments or contacting your children's schools.

### UNACCEPTABLE INTERNET/E-MAIL USE

Examples of unacceptable Internet/E-mail use include, but are not limited to, viewing, sending, creating, and/or downloading any information that:

- A. Violates the rights of any other person, including the right to privacy.
- B. Contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or illegal material.
- C. Violates agency or departmental regulations prohibiting sexual harassment, and/or discrimination.
- D. Restricts access, reduces productivity, inhibits or impacts network performance of DCSS electronic resources, including, but not limited to:
- Playing games.
  - Engaging in on-line chat groups.
  - Uploading or downloading files for personal use.
  - Accessing streaming audio and/or video files for personal use.
- E. Encourages the use of controlled substances.
- F. Utilizes the system for any illegal purpose.
- G. Automatically forward E-mail to mailboxes outside the control of DCSS, including to your home, unless you have authorization for remote access to the DCSS network, as such action may result in the unauthorized disclosure of confidential information.
- H. Transmit material, information, or software in violation of any local, state or federal law.
- I. Conduct any political activity.
- J. Conduct any unapproved fundraising or public relations activities.
- K. Operate a personal Web Server or make available any Internet services using such server.
- L. Engage in personal business transactions or any activity for personal gain.

- M. Use department records for private gain, or divulge confidential information or records unless officially authorized to do so.

If you are using the Internet and a website appears containing offensive, sexually explicit and/or inappropriate material, the DCSS Help Desk should be contacted and provided the Universal Resource Locator (URL), e.g., <http://www.whoareyou.com>. This will allow DCSS staff to block inbound traffic from the site in the future. Also, because DCSS can monitor, log and/or recover all network activity with or without notice, voluntarily providing this information will remove any questions and/or concerns about why the site was accessed if network activities are audited or reviewed.

### E-MAIL RETENTION

E-mail items shall not be retained longer than necessary for business purposes.

It is critical that only appropriate E-mail records be stored. Keep only those records required to comply with state or federal statutes and regulations and save them as a word processing document or in some other non E-mail format, such as, spreadsheets, database file or a hard copy.

#### **Rules**

- A. The E-mail system will automatically delete messages from an E-mail user's inbound file ("Inbox"), outbound file ("Sent Items"), and deleted file ("Deleted Items") after ninety (90) days.
- B. To retain business items beyond the 90-day timeframe, users should remove business items from the "Inbox" and "Sent Items" within ninety (90) days. E-mail items retained for business purposes should be stored in another folder, file, or on paper. A user who retains an E-mail item should delete it when it is no longer necessary for business purposes. An E-mail item retained for business purposes is an electronic record subject to the provisions of the California Records Management Program.
- C. Nonessential Items: Users should delete nonessential items on an ongoing basis.
- D. Backup Retention: E-mail Administrators must destroy E-mail backups sixty (60) to sixty five (65) days from the date the data was backed up.

## Email Policy Exceptions

Exceptions to the above policies may be needed in specific situations. Any exceptions to the above policies will only be permitted with express permission of the DCSS Chief Information Officer, and Information Security Officer (ISO).

## ROLES AND RESPONSIBILITIES

Role	Responsibility
Employee	<ul style="list-style-type: none"> <li>A. Conduct all Internet and/or E-mail activities in a professional, lawful and ethical manner, including the use of and development of content for the Internet.</li> <li>B. Any confidential information sent through the Internet and/or E-mail could be intercepted, modified, misdirected, or destroyed by unauthorized persons if adequate access controls are not in place. Be sure the E-mail identifications (ID) you use are for the intended recipient(s). Two or more individuals may have similar mail ID's.</li> <li>C. Employees shall take every precaution to ensure the security of information. Confidential information may be transmitted via Internet and/or E-mail only when encryption, authentication, and/or any other DCSS ISO approved security schemes and/or policies are used to ensure that data is secured and made available to appropriate and intended recipients only.</li> <li>D. The downloading of any executable software is prohibited unless done with case-by-case knowledge and approval of the DCSS Chief Information Officer and/or the ISO. The primary reason for this is because viruses are frequently spread through downloaded software and files and may have an undue effect on workstation and network performance.</li> <li>E. DCSS employees may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law.</li> </ul>
Technology Services Division	<p>Employees should have no expectation of privacy except for personally identifiable data in accordance with requirements of the Information Practices Act of 1977. The Technology Services Division will monitor Internet and E-mail use for compliance with this policy. The department also has the right to access and provide the contents of employee E-mail messages to law enforcement or other officials during the course of a legal investigation. Records of Internet and E-mail activity may exist in system files long after they have been deleted and the records can be recovered by the state at a later date.</p>

### LIABILITY

The employee should be aware that they access the Internet at their own risk and the department is not responsible for any material viewed or downloaded or for any damages employees may suffer related to their use of DCSS electronic information resources, whether such damages are incidental, consequential or otherwise. This includes, but is not limited to, data lost as a result of network and other system delays or interruptions or the erroneous or non-delivery of data caused by negligence, errors, or omissions. Employees must recognize that the use of DCSS electronic information resources is a privilege and that policies implementing usage are requirements that mandate adherence. DCSS employees are further cautioned that Internet pages may include offensive, sexually explicit, and inappropriate material.

### CONTACT INFORMATION

Additional information or questions regarding this policy should be directed to Rebecca Stilling, Deputy Director, Technology Services Division, at 464-5472.

### EFFECTIVE DATE

This overview is to remain in effect until rescinded by an executive level office, i.e. Department Director or designee. For questions regarding updates and/or revisions to this policy, please contact the Policy and Procedure Unit at 464-5792 or email [DCSSPolicy&Procedures@dcss.ca.gov](mailto:DCSSPolicy&Procedures@dcss.ca.gov).