POLICY OF THE SUPERIOR COURT OF CALIFORNIA,
COUNTY OF ORANGE

TITLE: **COURT EMPLOYEE INFORMATION TECHNOLOGY SYSTEMS POLICY**

POLICY: The Orange County Superior Court's (OCSC) Information Technology Systems provide essential tools for the conduct of Court business. As with all other facilities and equipment, the Court's Information Technology Systems are public property and must be managed in a manner that maintains the integrity and security of Court records, the confidentiality of sensitive information and data, and the public's trust and confidence.

By accepting access to the OCSC's Information Technology Systems, Court employees agree to abide by all applicable policies and procedures.

DEFINITIONS:

"Information Technology Systems" and "systems" includes all computer, telephone, and broadcast media hardware (including peripherals), software applications and data (including electronic and voice mail), networks, network connections, Internet, text messages, documentation and other capabilities that process, transfer, or store data which are owned or provided by the Court.

"Court employees" include paid and unpaid interns, non-employees who work in some capacity for the Court, consultants, vendors, volunteer temporary judges, and other users granted access to the Court's Information Technology Systems.

This policy does not apply to Judicial Officers or Superior Court Commissioners, who are governed by the Judicial Officer Information Technology System Policy.

PROCEDURE:

1. Confidentiality and Public Trust

a. Employees should have no expectation of privacy in network activity or in the use of any Court Information Technology Systems, including e-mail, text messages and Internet communications

and uses.

b. Court Information Technology Systems do not provide a public forum, and the Court maintains the right to limit and /or proscribe content and use.

c. The Court has the right to remove inappropriate content, data and software displayed, stored on, or sent over Court Information Technology Systems.

2. Security

a. Corrupted or infected files or data obtained over the Internet (including external e-mail) pose a threat to the security of the Court's network and, therefore, to the Court's essential operations. Accordingly, network activity (including e-mail, internet usage, shared drives) may be monitored at any time and without notice. Monitoring may include routine maintenance and backup, routine security and virus scanning, and emergency responses to threatened or actual breaches of security.

b. Anti-virus and scanning software designed to detect and cleanse incoming data and files, as well as detect and not deliver certain inappropriate data and files, are installed and must not be tampered with.

c. Instant Messenger programs that have not been installed or supported by the Court present an unacceptable risk to the security of the Court's Information Technology Systems, as they may bypass firewalls and virus scanners. Under no circumstances may external Instant Messenger programs be installed or downloaded. Court Technology Systems (CTS) will remove illegally installed or downloaded Instant Messenger programs, and the user will be responsible for reimbursing the Court for costs to remove the Instant Messenger programs and repair or restore the Court system.

d. Other than court-issued mobile systems, hardware and equipment must not be removed from assigned court locations and must be accessible by CTS personnel at all times. Do not store hardware or equipment in locked drawers, cabinets or offices for which there is no master key or pre-arranged access.

3. CTS Limited Access

a. Access to and review of a specific user's systems activity beyond monitoring, maintenance,

backup, routine security or virus scanning, emergency response, or the removal of inappropriate content and data displayed or stored on and sent over Court Information Technology Systems (as described above) requires authorization by both the Chief Technology Officer and Human Resources Director, or their respective designees.

4. Responsibility and Ethics

All users of the Court's computer system shall:

a. Protect the integrity and security of the Court's Information Technology Systems.

b. Protect the integrity and security of public Court records.

c. Protect sealed and confidential Court records and the confidentiality of sensitive and/or personal data and information in public Court records.

d. Maintain the operational efficiency of the Court's systems.

e. Obey licensing and copyright laws, regulations, and policies.

f. Adhere to a high standard of personal ethics in the use of electronic information, data, and materials.

g. Respect the confidentiality of others. Think before including personal information in e-mails, sharing or forwarding e-mails, or including non-Court addressees on document drafts or in-court electronic communications.

h. Not engage in practices that degrade or impair the performance of the Court's Information Technology Systems. This includes overloading systems with excessive data, executable programs, or voluminous attachments.

i. Not damage or alter hardware, software, or other components of the Court's Information Technology Systems.

j. Notify management and/or CTS staff and/or Human Resources immediately of possible security breaches and possible misuse of Information Technology Systems.

5. Internet Access

a. Internet access is authorized only for several categories of Court users and unauthorized access is prohibited.

b. Internet access may be restricted to approved websites, and accessing unapproved websites is

prohibited. Requests to expand the list of approved websites must be submitted to, and approved by, the Chief Technology Officer.

6. Incidental Personal Use

Incidental personal e-mail, internet access (where granted), and use of Windows-installed games is permitted on staff's "own" time, not during court business hours. In no circumstances may court employees play computer games within view of the public including during break periods.

7. Inappropriate and Prohibited Uses and Conduct

The following prohibited conduct is cause for loss of access privileges and/or disciplinary action, including termination. **No Court employee may use Court Information Technology Systems to:**

a. Violate any state or federal law or regulation;
b. Access, transmit, receive, or display inappropriate content or data, including defamatory, false, abusive, obscene, pornographic, sexually explicit, threatening, racist, sexist, harassing or illegal material;
c. Promote any political, union, religious, or other ideological activities or causes;
d. Conduct a personal business or the business of for-profit or nonprofit organizations;
e. Solicit funds;
f. Send or receive "chain" letters/mail, regardless of the subject;
g. Access fee-based websites or programs using Court funds or Court credit cards.

8. Use of Smart Phones/Personal Computers for Court Related Business Outside of Normal Work Hours

a. CTS assistance for setting up the Court's email system to smart phones or personal computers will only be provided to those employees who are expected to be available outside of working hours.
b. Non-exempt employees covered by the FLSA are not required or expected to use smart phones or personal computers outside of normal work hours to work on court related business. If the need arises to conduct work on a smart phone or personal computer outside of normal work hours, pre-approval should be obtained from management and any time worked must be accurately reflected

on your timesheet.

9. Unauthorized Access or Browsing

a. Accessing a Court Information Technology System, including terminals, PCs, and telephones, under another user's ID and/or password is prohibited.

b. Sharing ID's and/or passwords is prohibited.

c. "Browsing" in any form (e.g., files, programs, databases) unrelated to a specific, legitimate court-related search is prohibited.

10. Unauthorized Installation or Downloading

a. Only CTS personnel may install or download software or programs (including personal software and programs neither owned or licensed by the Court).

b. Requests for the installation or downloading of non-court-acquired or licensed hardware, software or programs must be submitted in writing to, and approved in writing by, the Chief Technology Officer. Blanket authorizations will not be issued. All such authorized software or programs must be installed by CTS. CTS will not, however, maintain or support non-court acquired or licensed software or systems. Under no circumstances will unlicensed software be authorized for installation or downloading.

c. Previously installed or downloaded hardware, software and programs that violate this policy will not be "grandfathered" under this policy; they must be approved and reinstalled by CTS personnel. The cost to repair any damage to the Court's Information Technology Systems as the result of an unauthorized installation or downloading is the user's responsibility.

Adopted: April 4, 2006

Revised: August 19, 2008
December 6, 2011
July 6, 2012
September 14, 2012

Approved by the Court Technology Committee