MANAGEMENT DIRECTIVE

DCFS INFORMATION SECURITY

Proper Use and Secure Transmission of E-mails

Management Directive #20-05

Date Issued:

☒ New Policy Release

□ Revision of Existing Procedural Guide dated

Cancels: None

PURPOSE

To establish a policy for proper and secure use and transmission of e-mails.

DEFINITIONS

EXHIBIT A – Information Technology and Security Definitions.

POLICY

The Department of Children and Family Services (DCFS) e-mail solution and software is an essential County communication resource and a privilege that shall be reasonably and adequately safeguarded and used for County business purposes only, ethically, professionally, as intended, and authorized.

To reduce risk of unauthorized or unnecessary discourse of County data and information, access, storage and transmission of data and information shall be authorized, encrypted as applicable, and limited to need-to-know basis and minimum necessary required to accomplish and fulfill the intended purpose or request.

DCFS Workforce shall:

a. Only use Department-provided e-mail account for County business purposes. Sending or receiving (including forwarding) County data via non-County provided or approved e-mail solutions (e.g., Gmail, Yahoo, iCloud mail) is prohibited;

b. Verify the accuracy of the recipient’s e-mail address prior to sending an e-mail. Extreme caution should be exercised to ensure outgoing e-mails are sent to the intended recipients with the recipient’s correct e-mail address;

c. Encrypt all outgoing e-mails containing sensitive/confidential information by using Department-provided and approved encryption solution. Placing the word “[Secure]” including brackets anywhere in the subject line will encrypt all outgoing e-mails (the word 'Secure' is case-insensitive);

d. Avoid placing any sensitive/confidential information in the subject line of an e-mail. Encryption will not encrypt the subject line; and

e. Immediately retract e-mails to non–intended recipients and report to DCFS Information Security Officer as an information security incident using one of the following methods:

   - Internal Services Department (ISD) eService Portal via: DCFS LAKids Intranet site Home page or http://sms.isd.lacounty.gov/cherwellPortal.

   - Contact ISD Help Desk at: (562) 658-1606 or (562) 940-3305.

No entitlement or expectation of privacy is conveyed to DCFS Workforce concerning their activities when obtaining or utilizing County or DCFS Information Assets including, without limitation, anything they possess, access, use, view, create, store, or transmit (send, receive or share). Such activities are also subject to litigation and electronic Discovery (eDiscovery). The Department has the right to administer, modify, revoke and/or restrict, monitor, log, store, make public, investigate, put a litigation hold, audit and/or review all activities of DCFS Workforce related to use or access of DCFS Information Assets and resources via authorized personnel at any time without notice or consent, including, without limitation, Internet usage and activities, electronic communications (e.g., e-mails, instant messaging sites, chat groups, newsgroups), data downloaded from or uploaded to the Department, files, data sets, databases, applications or systems.

APPLICABILITY

This policy applies to all DCFS Workforce.

COMPLIANCE

DCFS Workforce who violate this directive may be subject to appropriate disciplinary action, up to and including discharge, as well as both civil and criminal penalties.
Non-DCFS Workforce, including, and without limitation, contractors, in violation may be subject to termination of contractual agreements, denial of access to County or DCFS resources, and other actions, as well as both civil and criminal penalties.

POLICY EXCEPTIONS

There are no exceptions to Information Security Management Directives and policies.

RESPONSIBLE DEPARTMENT

Department of Children and Family Services

REFERENCE

DCFS Management Directive (MD) 20-01 – Use of DCFS Information Assets