STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, August 20, 2025

CF OPERATING PROCEDURE
NO. 50-22

Systems Management

# ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

This document describes the Department's policy for the use of DCF-owned information technology resources (e.g., desktop computers, laptops, tablets, smartphones, and associated devices), including but not limited to the handling of information in any digital format or medium (e.g., email, internet usage, text messaging). Department system users shall adhere to the acceptable use policies (AUP) and procedures outlined herein to minimize the Department's exposure to risks (e.g., virus attacks, compromise of network systems and services, and legal issues).

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Revisions to CFOP 50-22 include, but are not limited to, paragraph 2-6, which establishes the Phishing Awareness training policy; paragraph 2-7, which ensures compliance with federal requirements; and paragraph 7-3, which clarifies the process for reporting suspected spam emails.

TABLE OF CONTENTS

## Chapter 1 - GENERAL

1-1. Purpose. This document describes the Department's policy for using DCF-owned/leased information technology resources (e.g., desktop computers, laptops, tablets, smartphones, and associated devices). The operating procedure also covers handling of information in any digital format or medium (e.g., email, internet usage, text messaging). Inappropriate use exposes the Department to risks which include but is not limited to virus attacks, compromise of network systems and services, and legal issues.

1-2. Scope. This policy applies to DCF employees and community-based providers connecting to the DCF network. The operating policy applies to all system users accessing DCF information technology resources at any location. The procedure outlines the acceptable use of Department information technology resources, the responsibilities of employees in ensuring the security and confidentiality of DCF information and data, including employee responsibilities toward a security event.

1-3. References.

a. Section 282.318, Florida Statutes (F.S.), "*State Cybersecurity Act*."

b. Section 501.171, F.S., "*Security of Confidential Personal Information*."

c. Section 112.313(6), F.S., Misuse of Position.

d. Section 812.014, F.S., Theft.

e. Chapter 815, F.S., "Florida Computer Crimes Act."

f. Chapter 119, F.S., "Public Records."

g. Chapter 60GG-2, Florida Administrative Code, "*Florida Cybersecurity Standards*."

h. CFOP 60-55, Chapter 1, Standards of Conduct and Standards for Disciplinary Action for Department Employees.

i. The Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) Version 2.2 Requirements.

j. Internal Revenue Services (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (11-2021).

k. Social Security Administration (SSA), Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, the SSA standards based on Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974.

l. 45 CFR Parts 160 and 164, Subparts A and C, "Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules."

m. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

1-4. Definitions. Refer to the Glossary of Acceptable Use Terms for terms relevant to the policy.

1-5. Review and Revision. This operating procedure will be reviewed and updated by the Department's Information Security Manager or delegate, annually or when a significant change occurs, whichever occurs first; refer to Appendix A: Policy Review and Revision.

## Chapter 2 – GUIDING PRINCIPLES

2-1. Enforcement. Violations of information security policies and procedures described herein but not limited to this operating procedure may result in loss or limitations on use of DCF IT resources, disciplinary action, up to and including termination of employment or contractual relationship, and referral for civil or criminal prosecution as provided by law.

2.2. Principle of Least Privilege. System users receive access to Department-owned/leased information technology resources based on the principle of least privilege, which ensures access is necessary to accomplish assigned tasks in accordance with DCF missions, business purposes, and operating procedure CFOP 50-2. Department data, information, and technology resources are for official Department business only, except as provided herein.

2-3. Proprietary Information. Department information and data remain the sole property of the Department, even if stored on electronic and computing devices owned by an employee or a third party.

2-4. Subject to Disciplinary Action. Inappropriate use of DCF information technology resources and the data contained therein will subject employees and system users to revocation of access and/or discipline up to and including termination of employment and possible criminal charges.

2-5. Exception Requests. Any requests for an exception to any portion of this policy must be in writing, approved by the employee's supervisor, and forwarded to the DCF Chief Information Officer (CIO) for review.

2-6. Training Requirement. Upon hire and then annually thereafter, all system users shall complete the DCF Security Awareness training course, which includes training on recognizing and reporting potential insider threat. In addition to annual training, Department employees must complete monthly automated awareness testing and training that reinforces emerging threats, phishing detection, and Department security policies. The Department shall also distribute quarterly awareness newsletters to employees, highlighting current threats, lessons learned from recent incidents, and practical security tips.

2-7. Role-Based Training. When applicable, system users shall complete role-based training before accessing information systems or performing assigned duties, including but is not limited to accessing Federal Tax Information (FTI) and Social Security Administration data. In addition, to specialized training for system users with but not limited to elevated (e.g., privilege) access and responsibilities.

## Chapter 3 - RULES OF BEHAVIOR

3-1. Information Resources Usage Restrictions. Access to the Internet, Intranet, smartphone, and email may be granted as part of DCF employment, by contract with DCF, or by legal agreement. DCF information system users must adhere to all applicable state policies, Department policies/procedures, Federal regulations, as well as State and local laws.

3-2. Permitted Personal Usage. DCF information system users may use DCF-owned resources to access the Internet for personal use during work and non-work hours, provided use is brief, the content is appropriate and the system user adheres to the guidelines.

3-3. User-Installed Software. Only Department approved software shall be installed on DCF IT Resources.

a. DCF information system users are prohibited from using the Department's Internet or email services to knowingly download or deliver software or data files that do not comply with CFOP 50-7, Statewide Office Automation Standards. All software downloads or installations must be approved in writing by authorized Office of Information Technology Services (OITS) staff, whether via email or in a DCF IT ServiceNow ticketing system. Violations of software license agreements or information services contracts by the unauthorized duplication of software, files, operating instructions, or reference manuals are prohibited.

b. Any software or files approved for downloading onto DCF IT resources become the property of the Department.

c. Any files or software approved for downloading and installation may be used only in ways that are consistent with license and copyright.

3-4. Resources/Data Protection. DCF information system users will safeguard sensitive and confidential information and data from unauthorized change, destruction, or disclosure.

3-5. Resources/Data Authorization. DCF information system users must obtain documented authorization before taking DCF IT resources or information away from an agency facility.

3-6. Resources/Data Violations. DCF information system users shall not attempt to access DCF IT resources and information they do not have authorization or explicit consent to access must obtain documented authorization before taking DCF IT resources or information away from an agency facility.

3-7. Device Restrictions. The Department prohibits privately owned devices from connecting to Department-owned IT resources without documented agency authorization.

3-8. Cybersecurity Mechanisms. DCF information system users are prohibited from disabling or modifying encryption, anti-virus protection, and firewall software configuration settings on Department-owned IT resources.

3-9. Multi-Factor Authentication (MFA). DCF information system users must use a DCF Virtual Private Network (VPN) secure encrypted tunnel from a remote network to the Department's network. All DCF employees must utilize a DCF-approved technology when remotely accessing the network through VPN or other means via multi-factor authentication.

3-10. System Use Notification. Department information system users shall acknowledge the Department's network warning banner per 50-2, which informs users of acceptable behavior, consent to monitoring, and penalties for violating policies and procedures. In addition, system users shall acknowledge an IRS-approved notification banner with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance to log on to or further access information systems containing FTI data.

3-11. Communication/Collaborative Devices. Department system users can leverage secure Department-approved communication including but not limited to (i.e., telephones using Voice Over Internet Protocol [VOIP], Microsoft (MS) Teams, and OneDrive) to take advantage of the following features, which include but are not limited to remote meeting devices, networked whiteboards, cameras, microphones, file storage (including collaboration on files), and application integration.

a. The Department prohibits remote activation of collaborative computing devices and applications with the following exceptions: users receive notification by signage of the presence of such devices; and

b. Provide an explicit indication of use to users physically present at the devices, for example, signals to users when collaborative computing devices and applications are activated.

c. For example, MS Teams, Department-approved application has a 'PEOPLE' icon which displays the participation status of meeting invitees: 'In this meeting' (active participants) and 'Other Invited' (invited but not in attendance). Staff shall limit informational sharing to individuals with a need and right to know to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants. In addition, users shall be aware of application settings (e.g., camera, microphone).

(1) By default, the camera setting is 'OFF,' and the microphone setting is 'ON.'

(2) Participants in collaborative computing sessions may adjust their camera and microphone settings by clicking on the appropriate icons.

(3) Camera and microphone settings default to 'OFF' if there are five or more active participants when a user clicks 'JOIN' to enter the meeting.

## Chapter 4 - MONITORING USE OF AGENCY IT RESOURCES

4-1. Privacy Expectations. Department information system users shall have no expectation of privacy in their use of DCF IT resources, including but not limited to documents created, stored, sent, received, or deleted on DCF IT resources, including all messages (e.g., voice, text, emails) sent and received via Department communication platforms, or any other DCF IT resource related activity. The use of DCF IT resources constitutes consent to monitoring activities with or without warning, and monitoring and auditing may occur without the employees' knowledge.

4-2. Monitoring/Auditing. The Department shall check, log, and/or audit DCF IT resource usage (e.g., Internet activity, VOIP, smartphone, email use). In addition, the Department shall inspect files stored on any network or local computer system, including removable media attached to Department IT resources.

4-3. Boundary Protections. The Department has installed firewalls, proxy servers, internet website blocking, reporting programs, and other control systems to assure the safety and security of DCF IT resources. Any DCF information system user who attempts to disable, defeat, or evade any Department security feature without appropriate documented exception authorization from the CIO may be subject to disciplinary action, including termination of employment.

## Chapter 5 - USE OF THE INTERNET ON DEPARTMENT IT RESOURCES

5-1. Personal Use. During non-work hours, such as lunch breaks or before/after scheduled work hours, system users may access the Internet for personal business via the Department network and DCF IT resources, provided such use is appropriate as described herein.

5-2. Acceptable Personal Usage. Department employees are responsible for exercising good judgment regarding the reasonableness of personal use. Personal usage shall have no impact on the following:

a. Business. Usage shall not interfere with or disrupt the expected performance of the employee's job duties.

b. Technical. Usage shall not consume significant amounts of DCF IT resources (e.g., bandwidth, storage) or compromise the standard functionality of the Department's information systems.

c. Fiscal. Personal use must not result in any additional cost to the Department.

5-3. Unacceptable Usage. The following activities are, in general, prohibited. Under no circumstances is a department employee authorized to engage in any illegal activity under local, state, federal, or international law while utilizing Department-owned resources. Examples of Internet activities that are inappropriate and may subject employees to disciplinary action and denial of access to all DCF IT resources, as well as termination of contract or other agreements, include but are not limited to the following:

a. Distributing malware into the network or servers.

b. Disabling or circumventing security controls.

c. Forging headers.

d. Providing information about, or lists of, DCF employees to parties outside the Department without appropriate authority or authorization.

e. Propagating (sharing or forwarding) chain letters.

f. Using DCF IT resources to harass, threaten, or abuse others.

g. Political campaigning or unauthorized fundraising.

h. Using DCF IT resources for personal profit, benefit, or gain.

i. Offensive, indecent, or obscene access or activities unless specifically required by job duties documented in the employee position description.

j. Any harassing, threatening, or abusive activity.

k. Any activity that leads to performance degradation.

l. Automatic forwarding of DCF email to external non-DCF email addresses.

m. Unauthorized, non-work-related access to chat rooms, political groups, singles clubs, or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal

drug paraphernalia, hate-speech, or violence; hacker website/software; and pornography or sites containing obscene materials.

5-4. Prohibited Websites. Although the Department may install filters to block access to inappropriate internet sites, not every inappropriate site can be blocked by a filter. The items above identify examples of inappropriate activities, and system users should apply careful judgment whenever using Department information technology resources to access the Internet. If a DCF information system user is connected unintentionally to a site that contains inappropriate material (e.g., sexually explicit), they must disconnect from that site immediately and notify their supervisor.

5-5. Social Networks/Media Sites. Social Networking Sites such as but not limited to LinkedIn, Facebook and X allow users to build virtual communities for communicating and sharing information. Before accessing these sites, refer to CFOP 50-25, Guidelines for Using Social Networking Sites and Social Media.

## Chapter 6 – REIMBURSEMENT OF UNAUTHORIZED TELEPHONE COSTS

6-1. Purpose. This operating procedure establishes Department policy for calls and data costs/fees incurred from unauthorized use of state telephones and owned or leased cellular phones.

6-2. Scope. This operating procedure applies to all Department employees, clients, residents, guests, visitors, contract personnel and other persons, all Department voice telecommunications systems, and instruments.

6-3. Reimbursement for Unauthorized Usage Costs/Fees.

a. Unauthorized use of the state communications network is prohibited and subject to disciplinary action per section 2-1. Cellular phones should only be used for the conduct of official state business when a conventional phone is not readily available. Billing options should be reviewed to determine that the most economical option is selected considering the specific usage requirements of the cellular phone user.

b. Personal use of State-owned or leased cellular phones on package minute plans should be discouraged. The Department prohibits staff from incurring collect (operator-assisted) and international costs/fees; if incurred costs/fees equal to or greater than $5.00 for the billing period, a form CF 762 (available in DCF Forms) shall be completed to calculate the charges.

c. Submit the completed and signed form CF 762 with the employee's personal check. The check is payable to the Department for associated international costs/fees, plus a $3.00 processing fee.

d. The use of the state telecommunications system or state cellular telephones to facilitate a crime or in violation of Department rules, operating procedures or policies is strictly prohibited and subject to disciplinary actions; refer to section 2-1. Third party calls (calls made from a non-Department of Children and Families number) may not be billed to the Department.

## Chapter 7- USE OF DEPARTMENT EMAIL AND TEXT MESSAGING

7-1. Public Records. Business and personal emails and texts sent from or received by the DCF email system and smartphone devices are public records. Emails and text messages containing exempt or confidential information remain public records but should be reviewed and appropriately redacted according to Florida Statute before being released.

7-2. Confidentiality Notice on Email. With supervisor approval, DCF employees may create and use a Confidentiality Notice signature block in Outlook for outgoing email messages sent from the Department to external recipients using this text:

> "CONFIDENTIALITY NOTICE: This email and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorized review, use, disclosure, or distribution is prohibited. If you believe you have received this message in error, please contact the sender and then destroy all copies of the original email."

7-3. Phishing/Report as Spam. Department staff should report emails received in the DCF email system that they suspect pose a malware threat to the Department's IT resources, even if they are uncertain. To report potentially harmful emails, right-click on the email, hover of 'Report', then select 'Report phishing' and complete the corresponding prompts. Next, delete the email from both the Outlook 'Inbox' and 'Deleted Items' folders, which is referred to as double-deleting. The Office of Information Technology Services (OITS) staff will receive a notification and begin analyzing the email content and origin. If necessary, the email will be quarantined or eradicated. Finally, staff will receive notification of the results.

7-4. Inappropriate Email/Text Usage. Examples of email and text messaging activities that are inappropriate and could subject employees to disciplinary action and denial of access to all DCF IT resources or termination of contract or other agreements include, but are not limited to:

a. Send or forward any email communication containing unencrypted confidential client, employee, or other Departmental information or data.

b. Sending or forwarding password and/or encryption key in the same communication containing sensitive client, employee, or other Departmental information or data. The password/encryption key shall be provided to the recipient separately via email, verbally, or other means.

c. Using DCF issued smartphone to send text messages (instant messaging, SMS Messaging, Pin messaging, videos) for non-work-related activities.

d. Participation in any email or text communication from a department or personal account on DCF IT resources by sending, forwarding, or storing any message:

(1) Which supports a particular religious preference, belief, or group.
(2) That is harassing, intimidating, threatening, or disruptive.
(3) That contains profanity or inappropriate language, including, but not limited to, sexually suggestive, sexually explicit, pornographic, obscene, or vulgar (including off-color jokes or images), or material that makes fun of or insults a person because of race, color, religion, gender, national origin, disability, marital status, or age.

(4) Related to gambling, weapons, illegal drugs or drug paraphernalia, terrorist activities, or violence.

(5) Directed toward a political party's success or failure, candidate for political office, political campaign, fundraising, or partisan political advocacy group.

(6) Any chain letter, email, or text message.

e. Using Department email or smartphone account to conduct activities concerning the employee's secondary employment and/or outside business or commercial activities, including sending, storing, or forwarding any message for personal gain or associating in any way with the employee's Department email account with an outside business or commercial activity.

f. Solicitations for activities that the State or the Department does not sponsor; including but is not limited to, the advertising or sale of personal property; announcing the sale of cookies, candy, magazines on behalf of an organization or individual; or promoting personal events (weddings, showers, or events not related to work). NOTE: Recognition of employment or retirement and ceremonies for employee award programs are State business-related functions.

7-5. Appropriate Use of Personal Email and Smartphone Accounts.

a. During non-work hours, such as lunch break or before/after scheduled work hours, system users may access their browser-based personal email (for example, Gmail or Yahoo) for personal use utilizing DCF IT resources, provided such use is not inappropriate as described herein. This privilege applies only to browser-based functionality; DCF employees shall not install personal email software on DCF IT resources.

b. Use of personal email and/or smartphone accounts is permitted as long as the emails/phone calls are brief, occasional, and appropriate for a work environment. Personal email/text messaging accounts are not to be used to:

(1) Send or receive Department work email (with or without attachments).

(2) Send or receive any email or text message with Department-owned files attached.

(3) Interfere with an employee's work performance or productivity.

(4) Interfere or disrupt any other DCF employee's work performance or productivity.

(5) Adversely affects the security or performance of the DCF network or other DCF IT resources.

(6) Disclose any Department-owned information or data.

## Chapter 8 – USE AND PROTECTION OF CONFIDENTIAL INFORMATION

8-1. Rules of Behavior. DCF information system users are responsible for maintaining the confidentiality and security of information as defined in this operating procedure and the required annual Security Awareness training (SAT), includes form CF 114 (available in DCF Forms and incorporated into DCF SAT). DCF information system users are not to use confidential information for any purpose that conflicts with State or Federal laws and requirements (e.g., curiosity or checking information on family members, neighbors, acquaintances, celebrities, committing identity theft, or using information for other personal gain or purposes).

a. Browsing confidential, sensitive, or personal Department information or data without a legitimate business need is prohibited and can result in disciplinary action up to and including termination of employment.

b. Employees shall notify their supervisor, the DCF Information Security Manager, or the DCF Inspector General's office if they become aware of any actual or suspected misuse of Department information or data.

c. Employees who violate confidentiality and security of information or data requirements will be subject to disciplinary and/or legal action per Department policy, and State and Federal law.

8-2. Types of Protected Data.

a. Social Security Administration (SSA). The Department functions as the Florida "state transfer component" to share social security information, including personally identifiable information (PII) with other State and Federal agencies that have agreements with the SSA.

b. Internal Revenue Service (IRS). DCF receives Federal tax information (FTI) for DCF eligibility determination purposes for individuals who apply for public assistance.

c. Florida Department of Health (FDOH). By agreement with FDOH, DCF has access to vital statistics information (i.e., birth, death, cause of death) for DCF child welfare, adult protective services, criminal justice coordination, and substance abuse and mental health.

d. Florida Department of Highway Safety and Motor Vehicles (FLHSMV). By agreement with FLHSMV, DCF has access to driver license information, including photographs, for DCF human resources, child protective investigations, adult protection investigations, and public assistance eligibility purposes.

e. Florida Department of Law Enforcement (FDLE). By agreement with FLDE, DCF has access to local, state, tribal, and federal criminal justice information.

8-3. Conditions of Use. The following describes general and specific conditions for using protected information: state and Federal law, the employee code of conduct, DCF security operating procedure CFOP 50-2, the Department security agreement for employees, training (i.e., Security Awareness Training, HIPAA), and individual applications for system access and this operating procedure. Department employees are responsible for ensuring they understand and comply with these conditions and should confer with their supervisor if they have any questions.

8-4. Transmission of Confidential Information. Generally, Department policy prohibits transmitting confidential information via email inside or outside the agency. If transmission is vital to DCF business,

the email or the file containing the information must be encrypted. Generally, the telecommunication lines used to send fax transmissions are not secure. System users must ensure that there is a trusted member at both the sending and receiving fax machines if confidential information is being transmitted and a cover sheet must be included which provides guidance to the recipient. If multi-functional printer-copier devices are used, the data must be encrypted in transit. The scanned information may not be stored on the local device.

8-5. Release of Information. The business information system owner will make any decisions relating to the release and distribution of information in any form (e.g., online inquiry, printed reports, CD, USB, microfiche, or any magnetic media). No information will be released without the owner's prior approval.

8-6. Sanctions and Other Consequences for Misuse. DCF information system users who unlawfully inspect, disclose, or otherwise misuse Department confidential information are subject to civil and criminal penalties under applicable State and Federal laws. DCF employees are also subject to disciplinary action by the Department. The table below shows the relevant DCF policies that cover the protected data received by DCF from other government business partners:

| Source | Data Type | DCF Policy |
|---|---|---|
| Social Security Administration (Federal) | Personally Identifiable Information (PII) | CFOP 60-5<br>CFOP 60-17 |
| Internal Revenue Service (Federal) | Federal Tax Information (FTI) | CFOP 50-2<br>DCF SOP S-4 |
| Florida Department of Health | Vital Statistics | CFOP 60-17 |
| Florida Department of Highway Safety and Motor Vehicles | Driver's license information and photos | CFOP 50-1 |
| Department of Health and Human Services (Federal) | Protected Health Information (PHI) | CFOP 60-17 |
| Florida Department of Law Enforcement (Federal) | Criminal Justice Information Services (CJIS) | CFOP 50-1 |

## GLOSSARY OF ACCEPTABLE USE TERMS

a. Automatic Email Forwarding. Defining a rule within an email account that forwards some or all emails received to another specific email account.

b. Bandwidth. Refers to how much data can be sent or received through a network connection given an amount of time.

c. Blocked Web Site. A website to which an authorized system administrator has disabled user access.

d. Brief and Occasional Use of Emails. Brief refers to the size of the message sent, received or downloaded. Usually, a message less than 300 words is considered brief. Occasional use means once-in-a-while for a short period of time, similar to the occasional use of the telephone for personal use or the occasional trip to a break room or vending machine.

e. Browsing of Data. To inspect, read or look through information with no specific work purpose.

f. Chain Letter Email. A message that attempts to induce the recipient to make a number of copies of the email and then pass them on to other recipients.

g. Chat Room. An interactive-by-keyboard online discussion about a specific topic hosted on the Internet.

h. Clean Desk.

i. Confidential Information and/or Confidential Data. Information exempt from disclosure requirements under the provisions of applicable state and federal law, e.g., the Florida Public Records Act, section 119.07, F.S.

j. Data. A collection of facts; numeric, alphabetic, and special characters processed or produced by an information technology resource and stored on a server.

k. Data Streaming (or Streaming Data/Multimedia). Streaming media technology allows real time or on-demand delivery of multimedia content (e.g., YouTube, Pandora, iHeart Radio). The media (video, voice, and data) is received in a simultaneous, continuous stream rather than downloaded all at once then displayed later.

l. Department Owned (also Department Managed). Any device, service, or technology owned, leased, or managed by the department for which a department through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

m. Employee. Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. For the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to DCF IT resources, including contracted staff and contracted vendor staff.

n. Exempt or Exemption. A provision of general law which provides that a specified record, or portion thereof, is not subject to the access requirements of section 119.07(1) or section 286.011, F.S., or section 24, Art. I of the State Constitution.

o. Firewall. A computer or computer software that prevents unauthorized access to Department data (as on the DCF network or Intranet) by outside computer users (private citizens using the Internet).

p. Inappropriate Email or Text Messaging. An email or text message and/or attachment that contains offensive material or material not suitable to the workplace. This material may include but is not limited to cartoons, messages, jokes, pictures, or stories that make fun of or insult a person because of race, color, religion, gender, national origin, disability, marital status, or age; fully or partially nude images; references to weapons or illegal activities; pornography; or messages designed to promote a particular religion or political activity.

q. Inappropriate (Internet) Website. A website that contains offensive material or material not suitable for the workplace. This material may include but is not limited to cartoons, messages, jokes, pictures, or stories that make fun of or insult a person because of race, color, religion, gender, national origin, disability, marital status, or age; fully or partially nude images; pornography; gambling sites; websites that promote illegal activities; sites that promote use of weapons or violence; or sites that utilize an excessive amount of bandwidth such as online radio, television, or movies for purposes other than work.

r. Information Security Manager (ISM). The person designated by the Secretary of the Department to administer DCF's information technology security program and serve as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with section 282.318, Florida Statutes, Chapter 60GG-2, Florida Administrative Code, and CFOP 50-2, Security of Data and Information Technology Resources.

s. Information Technology Resources (IT Resources). Information and data processing hardware (e.g., desktop computers, laptops, tablets, smartphones, and associated devices), software (e.g., open-source, freeware, etc.), services (e.g., supplies, personnel, facility resources, maintenance, training, etc.), and other related resources.

t. Malware. Programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy, exploitation, unauthorized access to system resources, and other abusive behavior. Malware is a general term used to mean a variety of forms of malicious, intrusive, or annoying software or program code, including viruses, worms, rootkits, and Trojan horses.

u. News Groups and Bulletin Board Service (BBS). Discussion groups on the Internet in which participants with similar interests leave messages or other information for participants to read related to the respective topic.

v. Non-Work Hours. Before and after the employee's supervisor-approved work schedule and during the employee's scheduled lunch.

w. Occasional Personal Use (of Email, the Internet, or Department Computer-Related Equipment). The infrequent or limited use of Department email or access of the Internet through the DCF network, and/or Department-owned computer-related equipment is permitted. For example, receiving or sending an email from/to your child's school to schedule a teacher conference is an

occasional and appropriate use of the Department's email. Similarly, reading an online article published by the local newspaper is an example of an occasional and appropriate use of the DCF network to access the Internet.

x. OITS. Florida Department of Children and Families, Office of Information Technology Services.

y. Privately-Owned Devices. Information technology resources that are not the property of the Department.

z. Social Networking Sites and Social Media. Primarily Internet based online communications channels dedicated to social networking, community-based input, interaction, content sharing (information, videos, images) and collaboration. Examples include LinkedIn, Facebook, Instagram, YouTube, TikTok, and Twitter.

aa. System Owner(s). The Department business unit that owns the data and has the primary responsibility for decisions relating to a particular information system's specification and usage.

bb. System Users. Any person or employee who, through State employment, contractual arrangement, charitable service, or any other service arrangement and with appropriate approvals, would have access to DCF facilities, DCF information technology resources, or DCF information and data for the purpose of conducting business or providing services.

cc. Text Messaging. An act of sending short, alphanumeric communications between two or more cellphones, pagers, or other hand-held devices, as implemented by a wireless carrier (e.g., instant messaging, SMS messaging, and PIN messaging).

APPENDIX A: POLICY REVIEW AND REVISION

| Version | DATE | ACTION TYPE | DESCRIPTION |
|---|---|---|---|
| 1.0 | 04/06/2022 | Annual Review and Revision (ARR) | Annual review completed; no substantive changes were made. |
| 2.0 | 09/13/2023 | ARR | Annual review completed and CFOP revised throughout to reflect the Department's current policy and procedures. |
| 3.0 | 12/03/2024 | ARR | Annual review completed; no substantive changes were made. |
| 4.0 | 05/12/2025 | Policy and Procedure Review | The Acceptable Use Policy, reformatted and revised to describe its acceptable use policy and procedures, includes reimbursement of unauthorized telephone usage costs and Appendix A: Policy Review and Revision chart |
| 5.0 | 08/21/2025 | Policy and Procedure Updates | Document revised due to policy and procedure changes, which include, but not limited to, paragraph 2-6, establish Phishing Awareness training policy; paragraph 2-7, revised to comply with federal requirements; and paragraph 7-3, to clarify the process for reporting suspected spam emails. |