ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

1. **Purpose.** This operating procedure describes the Department’s policy for the use of DCF-owned information technology resources (e.g., desktop computers, laptops, tablets, smartphones and associated devices). The operating procedure also covers the handling of information in any digital format or medium (e.g., email, internet usage). Inappropriate use exposes the Department to risks including virus attacks, compromise of network systems and services, and legal issues.

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

3. **References.**
   d. Chapter 74-2, Florida Administrative Code, “Florida Cybersecurity Standards.”
   e. DHHS CMS MARS E 2.0 Requirements.
   f. IRS Publication 1075, Rev. 11-2016.
   g. SSA Information Security Safeguards Requirements document; 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.

4. **Definitions.**
   a. **Automatic E-mail 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 E-mails.** 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 E-mail.** 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. **Confidential Information.** Information exempt from disclosure requirements under the provisions of applicable state and federal law, e.g., the Florida Public Records Act, s. 119.07, F.S.

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

j. **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.

k. **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.

l. **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 s. 119.07(1) or s. 286.011, F.S., or s. 24, Art. I of the State Constitution.

m. **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).

n. **Inappropriate E-Mail.** An email 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.

o. **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.

p. 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 §282.318, Florida Statutes, and Chapter 74-2, Florida Administrative Code.

q. Information Technology Resources (IT Resources). Information and data processing hardware (including desktop computers, laptops, tablets, smartphones and associated devices), software and services, supplies, personnel, facility resources, maintenance, training, or other related resources.

r. 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.

s. 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.

t. Non-Work Hours. Before and after the employee’s supervisor-approved work schedule and during the employee’s scheduled lunch.

u. Occasional Personal Use (of e-mail, 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. 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.

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

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

x. Social Networking Sites and Social Media. Social media are 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 and Twitter.

y. 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.

z. 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.
5. **Policy Statement.**

   a. System users are provided access to Department owned information technology resources for DCF business purposes. Except as provided herein, all DCF data, information, and technology resources shall be used only for official Department business.

   b. DCF information and data remains the sole property of the Department even if stored on electronic and computing devices owned by an employee or a third party.

   c. 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, as well as possible criminal charges.

   d. 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.

   e. All system users shall complete the DCF Security Awareness training course upon hire and then annually thereafter.

6. **Basic Principles.**

   a. Access to the Internet, Intranet, and email may be granted as part of DCF employment, by contract with DCF, or by other legal agreement. DCF information system users must adhere to all applicable state policies, Department policies and procedures, Federal regulations, as well as State and local laws.

   b. 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 contained herein.

   c. Only Department approved software shall be installed on DCF IT Resources.

      (1) DCF information system users are prohibited from using the Department’s Internet or email services to knowingly download or deliver software or data files. All software downloads or installations must be approved in writing by authorized OITS staff, whether via email or in a DCF Statewide Help Desk ticket. Violations of any software license agreements or information services contracts by the unauthorized duplication of software, files, operating instructions or reference manuals is prohibited.

      (2) Any software or files approved for downloading onto DCF IT resources becomes the property of the Department.

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

   d. DCF information system users will protect DCF information and data from unauthorized change, destruction, or disclosure, and will safeguard sensitive and confidential information and data.

   e. DCF information system users will not attempt to access DCF IT resources and information to which they do not have authorization or explicit consent to access.

   f. DCF information system users must obtain documented authorization before taking DCF IT resources or information away from an agency facility.
g. No privately owned devices shall be connected to Department-owned IT resources without documented agency authorization to do so.

h. DCF information system users are prohibited from disabling or modifying the configuration of encryption software, anti-virus protection, and firewall software on Department-owned IT resources.

7. Monitoring Use of Agency IT Resources.

a. The Department may check, log, and/or audit Internet activity, email use, and the use of DCF IT resources. DCF information system users shall have no expectation of privacy in their use of DCF IT resources, such use constitutes consent to monitoring activities with or without warning, and monitoring and auditing may take place without the employee’s knowledge.

b. The Department may inspect files stored on any network or local computer system, including removable media attached to Department IT resources. DCF information system users shall have no expectation of privacy in regard to documents created, stored, sent, received, or deleted on DCF IT resources (including all email sent and received via the DCF email system), or any other DCF IT resources related activity.

c. 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, up to and including termination of employment.

8. Use of the Internet on Department IT Resources.

a. During non-work hours, such as lunch break or before/after scheduled work hours, system users may access the Internet for personal use by means of the Department network and DCF IT resources, provided such use is appropriate as described herein.

(1) Personal use by a DCF employee must not interfere with or disrupt the normal performance of the employee’s job duties.

(2) Usage must not consume significant amounts of DCF IT resources (e.g., bandwidth, storage) or compromise the normal functionality of the Department’s information systems.

(3) Personal use must not result in any additional cost to the Department.

b. Examples of Internet activities that are inappropriate and may subject employees to disciplinary action and all DCF IT resource users to denial of access, as well as termination of contract or other agreements, include but are not limited to the following:

(1) Distributing malware into the network or servers.

(2) Disabling or circumventing security controls.

(3) Forging headers.

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

(5) Propagating (sharing or forwarding) chain letters

(6) Using DCF IT resources to harass, threaten, or abuse others.
(7) Political campaigning or unauthorized fundraising

(8) Using DCF IT resources for personal profit, benefit, or gain.

(9) Offensive, indecent, or obscene access or activities, unless specifically required by job duties documented in employee position description.

(10) Any harassing, threatening, or abusive activity

(11) Any activity that leads to performance degradation.

(12) Automatic forwarding of DCF email to external non-DCF email addresses.

(13) 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 web-site/software; and pornography or sites containing obscene materials.

c. 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-owned 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.

d. Social Networking Sites such as LinkedIn, Facebook, and Twitter allow users to build virtual communities for communicating and sharing information. See CFOP 50-25, Guidelines for Using Social Networking Sites and Social Media, prior to accessing these sites.

9. Use of E-Mail. Business and personal emails sent from or received by the DCF email system are public records. Emails containing exempt or confidential information remain public records but should be reviewed and appropriately redacted pursuant to Florida statute before release to the public.

a. Confidentiality Notice on E-Mail. 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.”

b. Emails received in the DCF email system that contain malware threats to the Department’s IT resources should be double deleted, which means deleted from the employee’s Inbox, then deleted from the employee’s Deleted Items folder in Outlook. If an employee is not certain whether an email contains malware or not, they should confer with their immediate supervisor and / or the DCF Statewide Help Desk.
c. Examples of email activities that are inappropriate and could subject employees to disciplinary action and all DCF IT resource users to denial of access or termination of contract or other agreements include, but are not limited to:

(1) Sending or forwarding any email communication containing unencrypted confidential client, employee, or other Departmental information or data.

(2) Participation in any email communication from a Department email account or personal Internet email account on DCF IT resources by sending, forwarding, or storing any message:

   (a) Which supports a particular religious preference, belief, or group.

   (b) That is harassing, intimidating, threatening, or disruptive.

   (c) 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.

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

   (e) Directed toward the success or failure of a political party, candidate for political office, political campaign, fund raising or partisan political advocacy group.

   (f) Any chain letter email.

(3) Using a Department email 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 the employee’s Department email account with an outside business or commercial activity.

(4) Solicitations for activities that are not sponsored by the State or the Department. This includes, but is not limited to, the advertising or sale of personal property; announcing the sale of cookies, candy, magazines, etc., on behalf of an organization or individual; or announcing 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.

(5) Using instant messaging, text messaging, SMS messaging or PIN messaging for Department business is prohibited.

d. Appropriate Use of Personal E-Mail Accounts.

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

(2) Use of personal email accounts is permitted as long as the emails sent are brief, occasional, and appropriate for a work environment. Personal email accounts must not be used to:

   (a) Send or receive Department work email (with or without attachments).
(b) Send or receive any email with Department owned files attached.
(c) Interfere with an employee’s work performance or productivity.
(d) Interfere or disrupt any other DCF employee’s work performance or productivity.
(e) Adversely affect the security or performance of the DCF network or other DCF IT resources.
(f) Disclose any Department owned information or data.

10. Use and Protection of Confidential Information.

a. DCF information system users are responsible for maintaining confidentiality and security of information as defined in this operating procedure as well as the required annual Security Awareness training and form CF 114 (available in DCF Forms). 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 identify theft, or using information for other personal gain or purposes).

(1) Browsing of 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.

(2) 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.

(3) Employees who violate confidentiality and security of information or data requirements will be subject to disciplinary and/or legal action in accordance with Department policy, and State and Federal law.

b. Types of Protected Data.

(1) 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.

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

(3) 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.

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

c. Conditions of Use. The general and specific conditions for using protected information and data are specified in state and Federal law, the employee code of conduct, DCF security operating procedure CFOP 50-2, the Department security agreement for employees, Security Awareness
training, HIPAA training, and individual applications for system access and this operating procedure. DCF employees are responsible for ensuring that they understand and comply with these conditions and should confer with their supervisor if they have any questions.

d. Transmission of Confidential Information. Generally, confidential information should not be transmitted via email inside or outside the agency. If transmission is vital to DCF business, then the email must be encrypted 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.

e. 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.

f. 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:

<table>
<thead>
<tr>
<th>Source</th>
<th>Data Type</th>
<th>DCF Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Administration (Federal)</td>
<td>PII</td>
<td>CFOP 60-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CFOP 60-17</td>
</tr>
<tr>
<td>Internal Revenue Service (Federal)</td>
<td>FTI</td>
<td>CFOP 50-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DCF SOP S-10</td>
</tr>
<tr>
<td>Florida Department of Health</td>
<td>Vital Statistics</td>
<td>CFOP 60-17</td>
</tr>
<tr>
<td>Florida Department of Highway Safety and Motor Vehicles</td>
<td>Driver’s license information and photos</td>
<td>CFOP 50-1</td>
</tr>
<tr>
<td>Department of Health and Human Services (Federal)</td>
<td>PHI</td>
<td>CFOP 60-17</td>
</tr>
</tbody>
</table>

11. Enforcement. Violations of information security policies and procedures 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.

12. Review and Revision. This operating procedure will be reviewed and updated no less frequently than every 12 months by the Department’s Information Security Manager

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

JOE VASTOLA
Chief Information Officer
SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Revised to meet Chapter 74-2, Florida Administrative Code compliance requirements.