


POLICY TITLE: Issuance and Use of Mobile Devices		PAGE 1 OF 6
	CHILD AND FAMILY SERVICES AGENCY Approved by: Raymond Davidson Agency Director Date: October 16, 2015	REVISION HISTORY:
	LATEST REVISION: October 16, 2015	

I. AUTHORITY	The Director of the Child and Family Services Agency (CFSA) adopts this policy to be consistent with the Agency’s mission and all applicable federal and District of Columbia laws and regulations, including § 1808 of Chapter 18 of the DC Personnel Manual, the Office of the Chief Technology Officer (OCTO) Sensitivity Policy (OCTO003.010), D.C. Official Code § 4-1303.06; the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and its implementing regulations (45 C.F.R. Parts 160 and Subparts A and C of 164)(“HIPAA”).
II. APPLICABILITY	This policy, as described, applies to CFSA workforce members who may also be referred to as users (workforce members are individuals that are 18 or older, full or part-time employees, contractors, volunteers, undergraduates, graduate interns, and externs) who are authorized to use CFSA equipment or facilities and have been provided with a user account to access CFSA resources.
III. RATIONALE	Mobile devices, such as smartphones, laptops, phablets and tablet computers, are important tools for the organization and CFSA supports their use to achieve its mission and its business goals. However, mobile devices also represent a significant risk to data security. Without appropriate security applications and procedures, mobile devices can be a conduit for unauthorized access to the organization’s data and IT infrastructure, putting confidential information at risk and also potentially exposing CFSA’s network to system viruses. CFSA has an obligation to protect information in order to safeguard the privacy interests of its clients, protected health information and reputation.
IV. POLICY	CFSA’s policy is to apply and maintain user accessibility requirements and workforce usage requirements for Agency-issued hardware (and software) that protect the confidentiality of clients.
V. CONTENTS	A. Official Use of Mobile Devices B. Issuing Mobile Devices C. Mobile Device Sensitivity D. Reporting Stolen, Lost or Damaged Mobile Devices E. Replacement of Mobile Devices F. Reimbursement and Replacement Cost G. Returning Issued Mobile Devices
VI. PROCEDURES	Procedure A: Official Use of Mobile Devices 1. All mobile devices are to be used for official business only. 2. CFSA employees are responsible for the security and maintenance (e.g., any updates, passwords, notifications mandated by the Agency) of

POLICY TITLE	PAGE NUMBER
Issuance and Use of Mobile Devices	Page 1 of 6

	<p>any issued equipment.</p> <ol style="list-style-type: none"> 3. Only software approved for use by CFSA’s Child Information Systems Administration (CISA) must be loaded onto mobile devices. If an Agency employee requires additional assistance, they must contact the CFSA Help Desk for assistance. 4. Agency issued mobile devices must only be used to fulfill employee job related responsibilities only. 5. Text messaging is an effective means of communicating with a client or other significant party (e.g., a legal guardian, guardian ad litem, assigned Assistant Attorney General, or a court official). However, texting for personal or non-work-related purposes is prohibited. 6. Mobile device and PDA (Personal Digital Assistant) phone bills are reviewed monthly by Facilities Management Administration (FMA) to monitor all calls, text messages, downloads, etc. that are suspected to be other than official government business or that are over the calling plan, and forwarded to the applicable program administrator (or designee) for review and validation. 7. The program administrator (or designee) responsible for initially approving the issuing of a mobile device is responsible for ensuring that the individual remits appropriate payment to cover the excessive or unauthorized usage outside of official government business. 8. If an employee purchases services or downloads mobile apps that fall outside of the contract calling plan, the employee is responsible for reimbursing CFSA for the full cost of the purchase. <i>Note: FMA must review all Calling Plans assigned to the user before requesting the user’s signature on the Mobile Receipt Form.</i> 9. Utilization of Electronic Protective Health Information (ePHI) for official Agency business use is permitted. The saving of ePHI on mobile devices and sending ePHI to unsecured networks outside of the district’s WAN is prohibited. <i>Note: for the purpose of this policy, ePHI shall be defined as individually identifiable health information transmitted and maintained by electronic media or any other form of medium, including paper or oral communication.</i> 10. For directory assistance services, all Agency employees must use a toll-free access number (1-800-373-3411). The conventional “4-1-1” directory assistance is a surcharged service, and all associated fees related to 4-1-1 calls must be paid by the Agency employee.
	<p>Procedure B: Issuing Mobile Devices</p> <ol style="list-style-type: none"> 1. Any Agency employee who is issued a mobile device from CFSA must first obtain a written approval to obtain the device from his or her deputy director or designee.

POLICY TITLE	PAGE NUMBER
Issuance and Use of Mobile Devices	Page 2 of 6

	<ol style="list-style-type: none"> 2. Before a new mobile phone is assigned, FMA must ensure that all pertinent SIM Card and IMEI data is recorded on the appropriate receipt form after which, the user must complete a new applicable Receipt Form <i>Note: if mobile devices are damaged or in need of repair due to a manufacture’s defect, the mobile device shall be wiped and removable storage mobile sanitized before sending to the service representative for action by FMA.</i> 3. To be fully operational and “user friendly”, certain mobile devices may require accessories (e.g., charger case). For those mobile devices the accessories will be included at no cost to the user. 4. CFSA employees shall contact the CISA Help Desk to determine whether training is required for mobile applications (apps). If training is required, the employee shall be responsible for scheduling training that is appropriate for that specific mobile device. 5. Agency issued devices will be equipped with a mobile device management (MDM) tool, which includes an encryption package. Employees shall not delete any application or software installed on the devices. <i>Note: All devices are required to have a security package in order to receive CFSA apps.</i> 6. Any software, data, or message on a CFSA-issued mobile device shall be the property of the District of Columbia Government. 7. All Agency employees who are issued a mobile device shall be required to sign the appropriate receipt and comply with the applicable contracted agreement.
	<p>Procedure C: Mobile Device Sensitivity</p> <ol style="list-style-type: none"> 1. Employees shall only access client information relevant to their assigned case. Non work-related use (e.g., streaming movies, browsing recreational websites) is prohibited. 2. Under no circumstances shall any CFSA employee save the following information on any mobile device unless the data is encrypted and password protected: <ol style="list-style-type: none"> a. FACES.net information b. Placement data c. Service provider information d. Client information 3. CFSA-issued devices shall never be left unsecured or unattended. 4. When using mobile devices off-site, Agency employees shall always be aware of their surroundings and take necessary precautions to ensure that no data is comprised, and ensure the physical security of the device to prevent devices from being stolen, lost, or damaged.
POLICY TITLE	PAGE NUMBER
Issuance and Use of Mobile Devices	Page 3 of 6

Procedure D: Reporting Stolen, Lost, or Damaged Mobile Devices

1. If a mobile device is stolen or lost, the employee must inform his or her supervisor and report the theft or loss to the Metropolitan Police Department (MPD) or the police department in the jurisdiction in which the mobile device was stolen or lost.
2. Within one business day from the date of the incident, the employee responsible for the mobile device submits a copy of the police report; along with a completed CFSA *Unusual Incident Report* (UIR) to the Agency's Office of Risk Management (ORM) (see [Employee Unusual Incident Reporting Policy](#)).
3. If a mobile device is damaged, the Agency employee must inform his or her assigned supervisor within one business day and reports the incident to ORM. ORM notifies the Facilities Management Administration (FMA).
4. Supervisors must contact CFSA's Information Security Officer (ISO) to initiate an investigation, in collaboration with the assistance of the HIPAA Privacy Officer.
Note: The supervisor must ensure that a CFSA Information Technology Incident Report Form is completed and forwarded to ORM and FMA.
5. During the investigation if it's determined that ePHI has been compromised, the ISO must notify the appropriate MDM to wipe the device and prevent data loss or intrusion and notifies the HIPAA Privacy Officer.
6. The ISO must complete a password reset, and notify the user.
7. The findings of the investigation shall be shared with the supervisor, ORM, and CFSA's Human Resources Administration (HRA).
8. Collectively, the ISO, ORM, and HRA shall determine if the Agency employee was careless in such a manner that the theft, loss, or damage of the mobile device could have been prevented.

Procedure E: Replacement of Mobile Devices

Note: Replacement of a mobile device following negligent loss is not guaranteed, and is subject to availability of a comparable mobile device.

1. Following completion of Procedure D, the ISO must complete a report to determine how to proceed with replacement of the mobile device.
2. A decision about whether a mobile device or its accessory shall be replaced shall occur within 72 hours or three business days from the date of the ISO's report.
3. If accessories are not returned with the mobile device, the user shall be responsible for the cost to replace the accessories.

POLICY TITLE

Issuance and Use of Mobile Devices

PAGE NUMBER

Page 4 of 6

	<ol style="list-style-type: none"> 4. Some mobile device accessories may not be replaceable unless covered by warranty for the contracted period that the Agency has established with the vendor. 5. If negligence is not substantiated as cause of the theft, loss, or damage of the mobile device, CFSA shall replace the mobile device at no cost to the employee. The employee shall be issued a new device as outlined in Procedure B.
	<p>Procedure F: Reimbursement and Replacement Cost</p> <ol style="list-style-type: none"> 1. In the event that the ISO's determines that employee negligence played a role in the loss, theft, or damage of the mobile device or its accessory, the employee shall reimburse CFSA for the total replacement costs of the device, and any software or hardware loaded onto the mobile device. 2. The cost for replacement of a mobile device or accessory shall be calculated according to the cost of the last procurement of said mobile device or accessory but not to exceed the original purchase price. The cost calculation shall equal the charge to the employee. 3. CFSA employees shall not privately purchase any mobile device or accessory as a form of replacement. 4. When reimbursement is required, the user shall be responsible for providing proof of reimbursement payment to FMA. 5. CFSA may request immediate payment in full for any stolen, loss, or damaged mobile device or any accessory issued to a CFSA employee. 6. If there are extenuating circumstances regarding stolen, loss, or damaged equipment or accessories, the employee shall have an opportunity to discuss the circumstances related to the degree of negligence with HRA or a designee. 7. Once payment has been received, CISA or FMA shall notify HRA of the replacement cost via interoffice memo.
	<p>Procedure G: Returning Issued Mobile Devices</p> <ol style="list-style-type: none"> 1. If a CFSA employee discontinues employment with CFSA, the employee must return any issued mobile devices, along with their associated accessories, before departure. The devices shall be delivered to FMA. 2. The CFSA mobile device returned to FMA for re-issuance must be wiped and removable storage sanitized before issuing to another employee. 3. If an issued mobile device or accessory is not returned, CFSA shall withhold an individual's paycheck or leave benefits for reimbursement until each issued mobile device is returned (District Personnel Manual, Section 2904). 4. If any mobile device or accessory is passed to another employee in a manner that is not in accordance with this policy's issuing guidelines, the employee that signed a receipt for the mobile device shall be

POLICY TITLE	PAGE NUMBER
Issuance and Use of Mobile Devices	Page 5 of 6

	<p>responsible and held liable for any damages or missing accessories.</p> <ol style="list-style-type: none"> 5. CFSA employees who transfer to other administrations where a mobile device is not required shall return the mobile device and associated accessories (if applicable) to FMA. 6. CFSA employees who fail to return mobile devices under the above-cited circumstances shall be responsible for the replacement cost. 7. When a CFSA employee returns any issued mobile device, the employee shall receive a receipt for the appropriate item(s).
--	---

POLICY TITLE	PAGE NUMBER
Issuance and Use of Mobile Devices	Page 6 of 6