NEW YORK STATE | Office of Temporary and Disability Assistance | Office of Children and Family Services

ANDREW M. CUOMO
Governor

SAMUEL D. ROBERTS
Commissioner

SHEILA J. POOLE
Acting Commissioner

Local Commissioners Memorandum

Section 1

Transmittal:	17-OCFS-LCM-14
To:	Local District Commissioners
Issuing Division/Office:	OCFS and OTDA Counsel's Offices
Date:	July 12,2017
Subject:	Establishing a Policy for the Use and Management of Mobile Devices by Local Departments of Social Services
Contact Person(s):	OCFS Counsel's Office (518) 473-8418 OTDA Counsel's Office (518) 474-9502
Attachments:	
Attachment Available Online:	

Section 2

I. Purpose

This Local Commissioners Memorandum (LCM) provides local departments of social services (LDSSs) with information and guidance regarding the use and management of mobile devices. For purposes of this guidance, "mobile devices" are defined as smartphones (e.g., iPhone, BlackBerry, various Android phones) and tablets (e.g., iPad). Laptops are specifically excluded from the scope of this LCM because the security requirements and controls available for laptops are considerably different from those for mobile devices. This guidance is intended to help LDSSs improve the management and security of mobile devices and to convey what a mobile device policy in a LDSS should include.

Please note that the New York State Office of Information and Technology Services has issued NYS-S14-009, *Mobile Device Security Standard*, available at http://www.its.ny.gov/sites/default/files/documents/mobile_device_security_standard_0.pdf and

NYS-S14-011, *Enterprise Mobile Management Technical Standard*, available at https://www.its.ny.gov/sites/default/files/documents/nys-s14-011.pdf.

The scope of these ITS policies is limited and does not encompass all issues identified by the New York State Office of Temporary and Disability Assistance (OTDA) and the New York State Office of Children and Family Services (OCFS).

LDSSs must seek the guidance of their attorneys and human resources experts when drafting or modifying their mobile device policy to address all legal obligations of the LDSS, including, but not limited to, compliance and litigation hold obligations. LDSSs must ensure that the use of any

applications on a mobile device is in conformity with the respective terms of service and that all users comply.

II. Background

LDSSs must ensure appropriate protection of, access to, and disclosure of confidential, private, personal, and/or sensitive information maintained in state and/or LDSS applications, systems, networks, and/or databases when permitting LDSS staff to utilize mobile devices.

Mobile devices are particularly susceptible to security threats for several reasons, including their small size, portability, connectivity protocols (e.g., Wi-Fi, Bluetooth, Near Field Communication, (NFC), hardware features (e.g., camera, microphone), and location services (e.g., Global Positioning System, (GPS). Because of the higher levels of threat exposure inherent to mobile devices, these devices may require more security and privacy protection measures than devices that are used only within an organization's facilities and networks. The wide range of available devices, operating systems, carrier-provided services, and mobile applications presents an additional security challenge to the confidentiality, integrity, and availability of information.

III. Essential Elements of a Mobile Device Policy in the LDSS

Each LDSS utilizing mobile devices shall develop and implement a mobile device policy. The policy must: (1) provide a comprehensive overview of the acceptable uses of a mobile device; (2) define what resources are permitted to be accessed from mobile devices (e.g., email); (3) specify what types of mobile devices can be utilized, (e.g., iPhone, iPad); (4) outline the degree of access that various classes of mobile devices may have; and, (5) specify how provisioning will be handled. Each LDSS shall make the mobile device policy available to OTDA and OCFS upon request.

An LDSS mobile device policy must include, but is not limited to, the following key elements:

a. Purpose

The purpose section of each mobile device policy shall emphasize that the LDSS is committed to protecting the confidentiality, integrity, and availability of confidential, personal, private, and sensitive information (PPSI). Furthermore, the LDSS mobile device policy should state that the LDSS is committed to maintaining compliance with all applicable state and federal laws, rules, regulations, as well as LDSS policies.

This section must indicate that the mobile device policy is intended to provide guidance and information to LDSS staff on the acceptable use of LDSS-issued mobile devices, as well as prohibit the use of personally owned (bring your own device, or BYOD) mobile devices for work purposes. This section must also include language stating that mobile device users must follow all necessary, technical, administrative, and physical measures to protect the security of mobile devices issued by the LDSS, protect sensitive data, and maintain compliance with state and federal requirements.

b. Scope and Definitions

This section must articulate who in the LDSS is permitted to utilize a mobile device.

c. Physical Security of Mobile Devices

This section must state that mobile device users must exercise due diligence and are responsible for maintaining the physical security of not only the mobile device(s), but the security and integrity of all information accessed, transmitted, or stored on the mobile devices. Suitable protective measures must be present, enabled, and used on all such mobile devices.

d. Technical Controls

This section should advise staff that the technical controls utilized by the LDSS provide protection from unauthorized access or misuse, facilitate detection of security or compliance violations, and support security and compliance requirements. Accordingly, users must be advised that they are not authorized to alter or disable security, physical, or compliance-based configurations, or any other portion of the standard mobile device image on LDSS-issued mobile devices. Users must likewise be advised that they are prohibited from tampering with or disabling any mobile device management solution.

Centralized mobile device management (MDM) technologies (e.g., MobileIron) provide a solution for controlling the use of mobile devices. In addition to managing the configuration and security of mobile devices, MDM technologies offer other features, such as encryption, secure access to enterprise computing resources, and policy enforcement. LDSSs are required to implement an MDM solution if they do not already have one in place.

e. User Controls

This section must articulate that authorized users of mobile devices consent to acceptable use provisions. This section will likely require specific provisions regarding specific mobile device capabilities, including, but not limited to, the following:

- Access to Third-Party Applications
- Global Positioning System (GPS)
- Bluetooth Technology
- Text Messaging
- Purging of the Mobile Device
- Updating the Mobile Device

f. Access Controls

This section should articulate a password requirement to limit and defend against unauthorized access and use. Basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out of the account, wiping the mobile device, etc.) must also be included.

g. Security Training

Educating users on the risks of mobile device use should be a normal part of user briefings and security awareness training. LDSSs should provide training to users that addresses threats and recommended security practices. The LDSS should require all authorized mobile device users to sign an agreement acknowledging receipt of the mobile device policy.

h. Network Security

This section must outline restrictions regarding connecting personally owned equipment (including, but not limited to printers, scanners, wireless devices, flash drives, etc.) to an LDSS-issued mobile device.

i. Encryption

Risks to the confidentiality and integrity of sensitive data, both at rest and in transit, can be reduced by using strong encryption technologies. Mobile devices must be encrypted. LDSSs should work with their IT staff to properly encrypt all LDSS-issued mobile devices. The mobile device policy must inform users that they are not authorized to alter or disable encryption. A mobile device that does not have encryption enabled may not be used to access, store, or transmit protected data.

j. Lost or Stolen Procedures

This section must detail the procedures to be followed if a mobile device is lost or stolen.

k. Compliance and Enforcement Handling

This section must assert that compliance with the mobile device policy is mandatory, and that any non-compliance with the policy may result in disciplinary action, civil liability and/or criminal penalties. Furthermore, the LDSS should highlight that it will take all appropriate measures to protect the security and confidentiality of its information assets and protected data.

l. Legal and Regulatory References

This section must convey that the mobile device policy addresses and incorporates compliance with a variety of federal and state statutory, regulatory, and policy requirements related to confidentiality, privacy, and information security, and should include a listing of the applicable requirements.

Issued By

/s/ Suzanne E. Miles-Gustave, Esq.
Name: Suzanne E. Miles-Gustave, Esq.
Title: Deputy Commissioner and General Counsel, OCFS
Division/Office: Office of Legal Affairs

/s/ Krista Rock
Name: Krista Rock
Title: General Counsel, OTDA
Division/Office: Office of Legal Affairs