



### OCFS Owned Devices

**Q. It is important that LAN Administrators report iPad reassignments to OCFS as soon as possible, using the following procedure:**

1. Local district or agency LAN Administrator sends email to for [comctrup@ocfs.ny.gov](mailto:comctrup@ocfs.ny.gov) providing the serial number of the device being transferred and the name and HSEN ID of received-from and transfer-to users. The transfer-to user must have responsibility for conducting/documenting casework contacts with children in foster care.
2. Asset Management emails an acknowledgement to the LAN Administrator pointing to the procedure (see Step 3) to re-set/re-assign the iPad. Asset Management also notifies End User Management to update the MobileIron records.
3. The LAN Administrator follows the following procedure to re-set/reassign the iPad.
  - a. Tap the Settings icon on the iPad home screen
  - b. Tap General in the menu to the left of the screen, then tap Reset (you need to scroll down a bit)
  - c. Here, you will have two options:
    - 1) "Reset All Settings" will restore all of your app settings to their original status (preferred so that personal data is removed from device)
    - 2) "Erase All Content and Settings" will reset all app settings and erase all of your data (photos, apps, bookmarks, music, etc.)
  - d. After selecting one of the two options above, your iPad will reboot
  - e. If you selected "Erase All Content and Settings," you will need to reconnect your iPad to iTunes in order to reactivate it.
4. The LAN Administrator or receiving worker re-installs the MobileIron application from the App Store. (See *Installing and configuring Mobile Iron on iPad* posted on [http://ocfs.state.nyenet/it/mobile\\_tech](http://ocfs.state.nyenet/it/mobile_tech).)

If you have any questions about this procedure, please contact [ocfs.dl.it.eum52@ocfs.ny.gov](mailto:ocfs.dl.it.eum52@ocfs.ny.gov).

**Q. Since the iPads are not on the Human Services Enterprise Network (HSEN), how is it possible to keep track of them?**

OCFS uses MobileIron which is a mobile device management (MDM) product. This tool enables OCFS to remotely determine that the standard profile is maintained on the OCFS-owned iPad and enables OCFS to locate and/or remotely wipe a device in the event it is lost or stolen. Each worker assigned an iPad must download the (free) MobileIron app from the App Store. (See *Installing and configuring Mobile Iron on iPad* posted on [http://ocfs.state.nyenet/it/mobile\\_tech](http://ocfs.state.nyenet/it/mobile_tech).)

**Q. May OCFS-owned iPads be shared by multiple staff?**

No, OCFS-owned iPads may only be assigned to one staff person at a time. Because the iPad will only accept a single passcode (that multiple people would share), it is not possible to electronically determine the identity of the person using it at any given time. This is an unacceptable security risk.



**Q. What has been the feedback from the iPad pilot project?**

At total of 132 casework staff from 19 local districts and voluntary agencies participated in the pilot. Approximately half responded to a user survey, reporting:

- It was easy to learn to use the iPad to perform work functions.
- The wireless keyboard is useful; the lack of it is a deficit.
- The iPad is most frequently used for progress notes (either directly into CONX or via a notepad).
- The iPads are also used to work on FASPs, PHRs, perform searches and maintain person data in CONNECTIONS as well as to access email, the internet, calendars, GPS and diversions for children.
- The iPads are having positive impacts on staff feeling they are more productive, getting progress notes done more timely and feeling less stressed.
- The touchscreen interface within CONNECTIONS can pose a challenge; a stylus can help.



**The following responses provide guidance to local district and agency administrators; casework staff should consult their supervisors in regard to district- or agency-specific policies that may be more restrictive.**

**Local District or Agency Owned Devices**

**Q. May a local district or agency purchase tablets such as Apple iPads or other mobile devices for use by casework staff to access OCFS applications (e.g., CONNECTIONS)?**

Yes, OCFS permits access to its applications and data from non-State owned devices, including desktops, laptops, tablets or smartphones. Mobile device users must only access OCFS applications through published Internet remote access links, **and not directly via the HSEN network**. The link to access CONNECTIONS is: <https://connections.ocfs.ny.gov>. It is necessary for users to first download Citrix Receiver, a free app from the App Store, the instructions for which are located in the LAN Administrator Guide located on the Mobile Access page of the OCFS Intranet and Internet.

NYS does not provide support for district- or agency-owned mobile devices. It is the district and agency's responsibility to make certain that the equipment is compatible with OCFS applications as well as install and maintain up to date anti-virus protection and firewall software on the device, wherever possible. All OCFS confidential information stored on or transmitted from a mobile device must be encrypted in accordance with the NYS Office of Cyber Security Cryptographic standard. This means district or agency policies in regard to use of any mobile device should include the requirement for a complex pass code which activates the encryption. For more detail specifically on Apple iPad encryption, see: [http://images.apple.com/ipad/business/docs/iOS\\_Security\\_May12.pdf](http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf).

Since there is greater risk to data integrity when casework staff use mobile technology to access OCFS applications while out of the office, district and agency administrators must make certain that staff are aware of and abide by the requirements contained in the terms and conditions that appear on the log-on banner for each OCFS application as well as the requirements contained in [CONNECTIONS Security](#)



[Awareness Message - May 2012 - Security Information for Remote Access to State Applications from Non-State Owned or Personally Owned Devices](#). These requirements include (but are not limited to):

- Adhere to all applicable Federal and State statutory and regulatory confidentiality requirements.
- Refrain from storing **any Personal, Private, or Sensitive Information (PPSI) or other confidential information on any district, agency or personally-owned devices, or on portable storage or web services, except as approved in advance by the OCFS Information Security Officer (ISO).**
- Physically protect the device when it is being used to access OCFS applications and provide an appropriate level of protection of password and account information used to access OCFS applications.
- Use only secure methods (that meet encryption requirements) to transmit confidential information. This includes use of wireless keyboards.

See the OCFS Telecommunications and Computer Use Policy (PPM 1900.00) for additional terms and conditions. Questions about specific security issues not enumerated herein or for reports of unacceptable use should be directed in writing to the OCFS Information Security Officer at [acceptable.use@ocfs.ny.gov](mailto:acceptable.use@ocfs.ny.gov).

**Q. Are there any recommended insurances district/agencies can purchase that would cover damages to district or agency owned devices?**

There are many different options for insurance depending on carrier. Through Apple support, Apple Care + is an option. More information is available at:  
<http://www.apple.com/support/products/ipad.html>

**Q. May a local district or agency that purchases Apple iPads use the OCFS profile on these devices?**

Yes. Districts and agencies may configure Apple iPads that they purchase in a way that meets their business needs. They may wish to consider using the Apple iPad device profile that OCFS has piloted. That profile template is located under Mobile Technology on the OCFS Intranet and Internet. The local district or agency should substitute its own name in the Identity section of the profile. The Mobile Technology page also contains:

- A LAN Administrator Guide that provides instructions on how to set up email and how to enable access to CONNECTIONS; and
- An iPad User Guide that all users should review before using an iPad to access OCFS assets. This guide provides security information about which each user should be aware.

**Q. May a local district or agency use Facetime?**

Yes, provided policies and practices described above to protect PPSI and other confidential information are adhered to. Users should also be aware that transmissions over Facetime are not fully secure and potentially susceptible to interception. Therefore, when using Facetime, users should not divulge client-identifying information (similar to emailing protocols).

**Q. Can emails sent from District/Agency iPads be password protected?**



The iPad's built-in email client supports encrypted email transfers over the Secure Sockets Layer (SSLVPN) protocol. The option to turn on SSL is in the "Advanced Settings" option under the "Account Information" screen for each of the email addresses that you have set up on the device. While SSL does not encrypt the email while it is on your iPad, it does encrypt email data as it is being sent over the public Internet between your iPad and your email server.

**Q. May local districts or agencies that purchase iPads utilize the mobile device management (MDM) solution that OCFS uses?**

Not at this time. OCFS currently uses MobileIron as an MDM solution and wishes to gain experience with it before considering the addition of other districts and agencies to it. OCFS will revisit this in the future. Districts and agencies that purchase iPads may wish to consider acquiring an MDM solution.

**Q. is there a government rate for purchasing iPads?**

Not at this time.

**Q. What apps from the Apple App Store has OCFS used for creating and editing Word documents or Excel spreadsheets?**

OCFS has worked with paid apps, such as DocsToGo and QuickOffice Pro for creating and editing Word documents, Excel spreadsheets and Adobe files. Reminder: users should not use any application to store confidential information on the device.

**Q. May I gain access to Word and Excel files located on my network (H:\) drive using an iPad or other privately-owned device?**

Currently, OCFS does not permit access to a user's H:\ drives because it requires a SSLVPN account. OCFS is trying to reduce the number of these accounts.

**Q. May I gain access to personal folders on Exchange using iPads?**

While it is possible to access your Exchange email Inbox via the Outlook Web Access (OWA) it is not possible to access personal folders that are stored on your H:\ drive. Note: users should be aware of the prohibition of using Active X to synch email between the device and the user's HSEN email account.



**The following responses provide guidance to local district and agency administrators; casework staff should consult their supervisors in regard to district- or agency-specific policies that may be more restrictive.**

**Individually Owned Devices**

**Q. May casework staff use their own tablets such as Apple iPads or other mobile devices to access OCFS applications (e.g., CONNECTIONS)?**

Yes, subject to several conditions and to the approval of the local district or agency that employs them. See the response to the first question under **Local District or Agency Owned Devices**.



Before accessing OCFS applications via personally owned mobile devices, users should first ask their supervisors if such use is permitted by their local district or agency. If this use is permitted, the user then must become familiar with the terms and conditions that appear on the log-on banner for each OCFS application as well as the requirements contained in [CONNECTIONS Security Awareness Message - May 2012 - Security Information for Remote Access to State Applications from Non-State Owned or Personally Owned Devices](#) located on the Security page as well as the *User Guide (revised) – Apple iPad Pilot* located under Mobile Technology on the Information Technology page of the OCFS Internet and Intranet.

Users of their own devices should, in addition to security requirements, understand that:

- Costs to procure, and/or maintain non-State owned devices will not be borne by NYS.
- NYS does not provide technical support for personally-owned equipment.
- When accessing OCFS applications, user’s activities are subject to monitoring; users should have no expectation of privacy.
- OCFS may revoke access to its resources and services from a personally-owned device should it determine that the access presents a risk to the agency’s mission.
- Users are responsible for making certain that the equipment is compatible with the OCFS application.
- OCFS make no warranties (expressed or implied) with respect to remote access services, and it specifically assumes no liabilities/responsibilities for:
  - Any costs, liabilities or damages caused by the user’s remote access to OCFS applications.
  - Any consequences of service interruptions or changes, regardless of whether these interruptions were within the control of OCFS or ITS.
  - OCFS and ITS provide remote access services on an “as is, where available” basis.
  - Any damage to equipment while accessing remotely. This includes, but is not limited, to hardware, software, deletion/loss of personal files, or virus damage.
  - Any third party (commercial) connectivity charges not authorized, ordered or supported by ITS. This includes bandwidth, connection support, and support of third party data communications equipment installed by vendors outside of ITS control.

### Miscellaneous

**Q. Are there any accessories that you feel are needed (other than the keyboard) so that the iPad would best function for on-call?**

A stylus and a mobile charger may be helpful; iPad compatible accessories can be purchased from many general department stores and directly from Apple.

**Q. Does OCFS recommend a particular type of protective case for the iPad that can be used in conjunction with a keyboard?**

OCFS is currently using the Targus case Model THD006US.

**Q. What is the average battery life when using the CONNECTIONS application on the iPad?**



Apple quotes the average battery life of an iPad 2 and iPad 3 at 10 hours when connected to Wi-Fi. Unfortunately there is no way to determine how use of CONNECTIONS will affect the battery life, as there are many different variables per user.

**Q. Is there a mobile app specifically for CONNECTIONS in development?**

OCFS and ITS are in the early stages of developing a mobile version of CONNECTIONS (mCONNECTIONS) for use on tablets that will support certain key functions that caseworkers most commonly perform on mobile devices in the field. OCFS/ITS is also developing an application for the secure transmission of pictures taken from smartphones and tablets for storage within CONNECTIONS. At this point, there is no time estimate for completing this effort. Workers can currently access CONNECTIONS on their mobile devices via: <https://connections.ocfs.ny.gov>.