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 or tablets. Such access is made through published Internet remote access links, **not directly to the HSEN network**. The link to access CONNECTIONS, ASAP, Webstar and the OCFS Intranet is: https://connections.ocfs.ny.gov.

NYS does not provide support for district- or agency-owned equipment. 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 transmitted or stored 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.

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 assets 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.state.ny.us.

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 on the Remote Access page of the OCFS/CONNECTIONS Intranet and Internet. The local district or agency should substitute its own name in the Identity section of the profile. The Remote Access 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 Apple iPads purchased by a local district or agency be used to access CONNECTIONS?

Yes. The LAN Administrator Guide located on the Remote Access page of the OCFS/CONNECTIONS Intranet and Internet provides instructions to download Citrix Receiver, a free app. Doing so will also provide access to other OCFS Citrix-based applications, including ASAP, Webstar, OCFS Intranet. Such access is made through published Internet remote access links, **not directly to the HSEN network**. The link is: https://connections.ocfs.ny.gov.

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

OCFS has worked with DocsToGo and Quickoffice Pro for creating and editing Word documents or Excel spreadsheets. Reminder: users should not use any application (other than CONNECTIONS, ASAP or Webstar) to store confidential information.

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.

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 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 on the Remote Access page of the OCFS/CONNECTIONS 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, OFT or ITS.
    - OCFS, OFT or ITS provides 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 OFT or ITS. This includes bandwidth, connection support, and support of third party data communications equipment installed by vendors outside of OFT control.