NYS OFFICE OF CHILDREN AND FAMILY SERVICES

Apple iPad Profile Used by OCFS for OCFS-Owned Devices

Local districts and agencies may configure Apple iPads that they purchase in a way that meets their business needs. The following is the Apple iPad device profile that OCFS has sucessfully piloted.

Identity

Name
Display name of the profile (shown on the device)
OCFS iPad

Identifier
Unique identifier for the profile (e.g. com.company.profile
OCFS

Organization
Name of the organization for the profile
OCFS

Description
Brief explanation of the contents or purpose of the profile
OCFS iPad Pilot

Security
Controls when the profile can be removed
With Authorization
Authorization password
••••••••

Substitute your own organization's name in the Idenity section

Web Clip

Label
The name to display for the Web Clip

Connections

URL
The URL to be displayed when opening the Web Clip

https://connections.ocfs.ny.gov

☐ **Removable**
Enable removal of the Web Clip

Icon
The icon to use for the Web Clip

Choose...

☐ **Precomposed Icon**
The icon will be displayed with no added visual effects

☑ **Full Screen**
Displays the web clip as a full screen application

Web Clip

Label
The name to display for the Web Clip

OWA

URL
The URL to be displayed when opening the Web Clip

https://mail.ny.gov/owa

☐ **Removable**
Enable removal of the Web Clip

Icon
The icon to use for the Web Clip

Choose...

☐ **Precomposed Icon**
The icon will be displayed with no added visual effects

☑ **Full Screen**
Displays the web clip as a full screen application

Restrictions

Device Functionality
Enable use of device features

- [x] **Allow installing apps**
- [x] **Allow use of camera**
  - [ ] **Allow FaceTime**
- [ ] **Allow screen capture**
- [x] **Allow automatic sync while roaming**
- [x] **Allow Siri**
- [ ] **Allow voice dialing**
- [ ] **Allow In-App Purchase**
- [ ] **Force user to enter iTunes Store password for all purchases**
- [ ] **Allow multiplayer gaming**
- [ ] **Allow adding Game Center friends**

Applications
Enable access to applications on the device

- [x] **Allow use of YouTube**
- [ ] **Allow use of iTunes Store**
- [x] **Allow use of Safari**
  - [ ] **Enable autofill**
  - [ ] **Force fraud warning**
  - [x] **Enable JavaScript**
  - [x] **Block pop-ups**

  Accept cookies
  Always

iCloud
Enable access to iCloud services

- [ ] **Allow backup**
- [ ] **Allow document sync**
- [ ] **Allow Photo Stream (disallowing can cause data loss)**

Security and Privacy
Enforce security and privacy policies

- [ ] **Allow diagnostic data to be sent to Apple**
- [x] **Allow user to accept untrusted TLS certificates**
- [x] **Force encrypted backups**

Content Ratings
Control access to apps and media

- [ ] **Allow explicit music & podcasts**

Ratings region
Sets the region for the ratings
United States

Allowed content ratings
Sets the maximum allowed ratings

Movies: Don't Allow Movies
TV Shows: Don't Allow TV Shows
Apps: Allow All Apps

Passcode

- [ ] **Allow simple value**
  Permit the use of repeating, ascending, and descending character sequences

- [x] **Require alphanumeric value**
  Require passcodes to contain at least one letter

8 **Minimum passcode length**
Smallest number of passcode characters allowed

2 **Minimum number of complex characters**
Smallest number of non-alphanumeric characters allowed

90 **Maximum passcode age (1-730 days, or none)**
Days after which passcode must be changed

5 minutes **Auto-Lock (1-5 minutes, or none)**
Device automatically locks when time period elapses

2 **Passcode history (1-50 passcodes, or none)**
Number of unique passcodes before reuse

1 Minute **Grace period for device lock**
Amount of time the device can be locked without prompting for passcode on unlock

10 **Maximum number of failed attempts**
Number of passcode entry attempts allowed before all data on device will be erased