## Protecting Your Portable Device

- Portable device users are responsible for the physical security of their portable devices at all times.
- Never leave your portable device unattended unless it is physically secured.
- When not in use, properly secure your portable device.
- Users must make certain that only authorized personnel have access to their portable devices, and the information stored on them.
- Do not view, discuss or process confidential information where it can be seen or heard by unauthorized persons.
- Always use a strong password to log on to your portable device so that it may not be easily hacked or guessed.
- Unless approved by OCFS, do not connect personally-owned equipment (printers, scanners, wireless devices, flash drives, etc.) to an OCFS portable device.

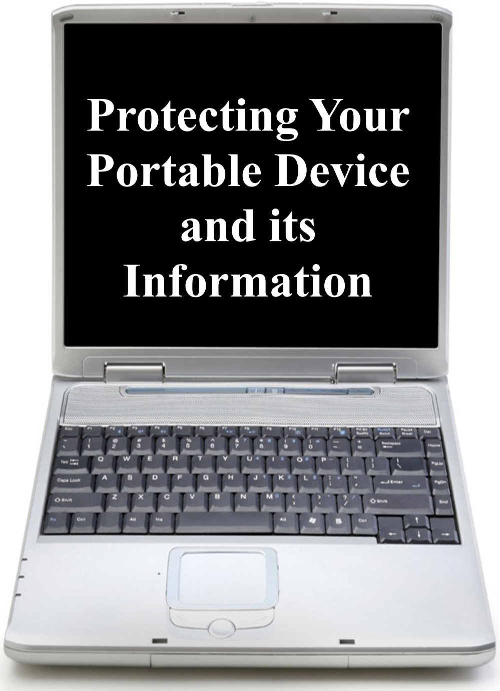
**Prepared by the OCFS Information Security Office (ISO)**

***New York State***
***Andrew M. Cuomo, Governor***

***Office of Children and Family Services***
***Gladys Carrión, Esq. Commissioner***

New York State
Office of
Children and
Family Services

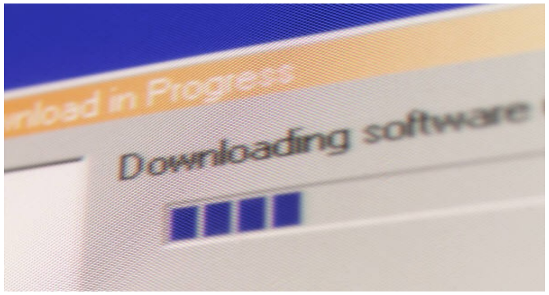
***July 2011***



# Protecting Your Portable Device and its Information

# OCFS Laptop and Other Portable Device Security

**New York State**
**Office of Children and Family Services**



**Why am I receiving this brochure?**
The reason you are receiving this brochure is to remind you of OCFS's portable device and data encryption requirements, and to update you regarding the following security awareness guidelines:

- Protecting OCFS's data and information.
- Laptop and Other Portable device security.

**Protecting OCFS's Data**
All staff within the OCFS or Local District workforce must protect OCFS's data and information from unauthorized access and maintain the confidentiality of OCFS's information.

This means…..

- Do not retain confidential information to your workstation or laptop's hard drive (including the computer's "My Documents" or Desktop area) after it has been transferred or uploaded to the State network.
- Do not connect personally-owned equipment (USB drives, MP3 players, i-Pods, etc.) to the OCFS network or computers (this includes vendors and contractors), unless approved by the OCFS Information Security Officer (ISO).
- Do not download unapproved software.
- Always report observed suspicious or questionable computer or network activity to your supervisor or LAN Administrator.
- Do not write down your password or share your password with anyone.

## Stay Protected - At a minimum, connect your OCFS-owned or issued laptop or other portable device to the HSEN monthly

In order to receive the latest anti-virus updates, software patches and system updates, you must connect your laptop or other portable device to the HSEN for a minimum of two consecutive hours each month, preferably overnight.

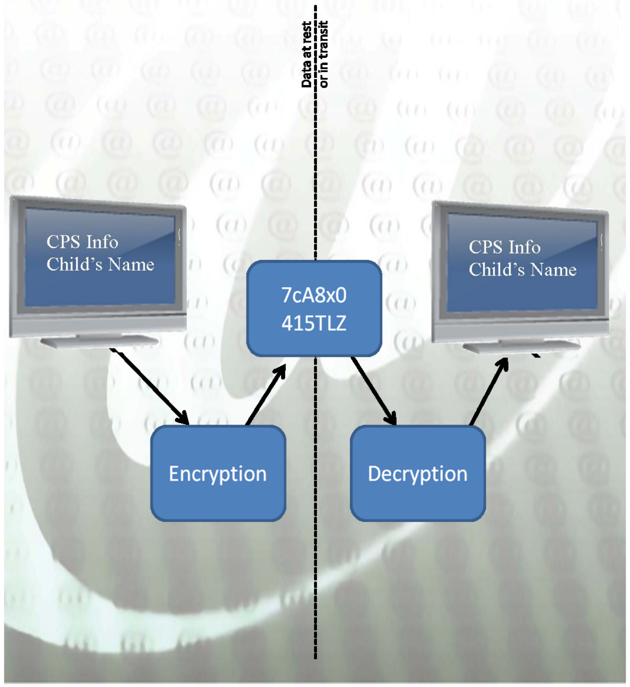
**Encryption**
Encryption is a process which transforms information into unreadable and unusable text while the information is at rest or in transit. In order to protect the confidentiality of information, OCFS requires all information stored on portable devices, including stored on portable media (such as USB drives) and in transit (data in transit to the network) to be encrypted.

Specifically, OCFS encryption requirements apply to:

- OCFS owned or issued Laptop computers and Portable Devices.
- OCFS owned or issued USB thumb/flash drives or other USB storage media.
- CDs/DVDs.
- OCFS owned or issued Personal Digital Assistants (PDAs), Blackberries.

E-mail containing confidential information must not be transmitted via the Internet (outside the HSEN) unless an OCFS approved encryption method is used.

If you are unsure whether your portable device is properly configured with an approved encryption package, please contact your LAN administrator.



# Encryption Protects OCFS's Info

**Laptop and Portable Device Security**

- An OCFS approved encryption package is required for all OCFS laptops and portable devices.
- Treat your OCFS issued laptop or portable device like cash; do not leave it unattended in a public location, in plain sight in your car or other unsecured area, and use a locking device, if available.
- Use only WiFi networks that you have been given permission to access. Use a virtual private network (VPN) and avoid using unsecured WiFi.
- Lock your laptop by using CTRL+ALT+DEL
- Avoid entering confidential information into your portable device while in public to prevent "shoulder surfing" or eavesdropping
- Report any loss or theft of your OCFS laptop or portable device to the police and submit the Lost/Stolen report form to your supervisor and LAN Administrator immediately.

**The security and confidentiality of OCFS's information is governed by various federal and state regulatory and statutory requirements.**

**If you have questions, please contact the OCFS ISO by e-mail at [Acceptable.use@OCFS.state.ny.us](mailto:Acceptable.use@OCFS.state.ny.us)**