

NYC Department of Education DIIT Office of Information Security Use of Personal Devices on DOE Network

Version 2.0

Last updated 5/14/2014

Purpose

This document governs the use of non-DOE devices on school-based networks.

This document does not describe logical or physical network separation such as Instructional vs. Administrative IP space as it is assumed that these would be Laptop, Slate, or Tablet devices connecting to the schools instructional wireless network.

Principals can authorize the use of a non-DOE device to connect to a school. Prior to authorizing such use, the Principal must ensure that the following conditions are understood and accepted, and that reasonable and appropriate measures are taken to ensure they are complied with. A copy of this document should be provided to the user.

- The non-DOE device must be used for an appropriate instructional or administrative purpose.
- Non-DOE devices will not be supported via standard support channels for hardware or software issues.
- Non-DOE devices are not warranted or covered under the school's PCS vendor agreement.
- The distribution and configuration of any SSID/WEP keys is the responsibility of the Principal or their school based designee.
- The configuration of any proxy settings specific to the DOE's network is the responsibility of the Principal or their school based designee.
- The device must have Anti-Virus software installed, and have up to date virus definitions.
- The device must have the latest Operating System critical patches.
- The device must not interfere with or disrupt standard operations on the school network.
- The device must adhere to existing web filtering rules. Modifications to filtering rules will not be made for non-DOE devices.
- The DOE assumes no responsibility for any issues encountered by, or damage to non-DOE Devices while used within the school.

While operating on the school network, users of non-DOE equipment should note that the device (*in addition to their activity on the network*) is governed by the DOE's [Internet Acceptable Use Safety and Privacy Policy](#) (IAUSP) and [Social Media Guidelines](#). A list of relevant technical resources is provided on the following page.

Technical Resource List

Internet Acceptable use and Safety Policy:

<http://schools.nyc.gov/RulesPolicies/InternetAcceptableUse/>

Social Media Guidelines

<http://schools.nyc.gov/socialmedia>

Requires DOE Logon

The Sandbox – Tech tools for employees of NYC DOE schools

<http://schools.nyc.gov/tech>

Request sites be filtered/unfiltered

<http://nycboe.net/Applications/Filtering>

Wireless Support Website:

<http://schools.nyc.gov/Offices/EnterpriseOperations/DIIT/Helpdesk/Wireless/XP.htm>

Employee Self-Service Password Reset:

<https://idm.nycenet.edu/selfservice>

Tech SharePoint (Requires DOE Logon):

<http://collaboration.nycboe.net/sites/FinanceAdmin/DIIT/operations/TechShare/default.aspx>

Free Anti-Virus Software (PC):

- Avast Free AV - <http://www.avast.com/free-antivirus-download>
- Microsoft SE - <http://windows.microsoft.com/en-US/windows/products/security-essentials>
- Avast 2014 - <http://www.avast.com/en-us/index>

Free Anti-Virus Software (MAC):

- ClamXav 2 (MAC) - <http://www.clamxav.com/>
- Sophos - <http://www.sophos.com/en-us/products/free-tools.aspx>
- Avast AV for MAC - <http://www.avast.com/free-antivirus-mac>