Florida Department of Education
WIRELESS TECHNOLOGY GUIDELINES

The Florida Department of Education is pleased to provide these wireless technology guidelines to assist schools and districts as they make their wireless infrastructure decisions to best meet the instructional and online assessment needs of their students in a classroom setting. Wireless technology is advancing at tremendous speeds which require educational institutions to maintain robust wireless infrastructures that can scale with the need for increasing bandwidth, security and mobility. The information in this document is intended to provide the Florida Department of Education's guidelines to assist in answering questions about whether the school's existing wireless infrastructures will support the future requirements for instruction and computer-based assessment administration as defined under the Florida Standards. These guidelines are not intended to recommend a brand or model of wireless hardware, or provide information concerning the physical deployment of wireless access hardware on your network. The Florida Department of Education recommends that a wireless site survey be part of any deployment effort.

Recommended Wireless Technology Specifications	
Institute of Electrical and Electronics Engineers (IEEE) Protocol Equipment Standard	802.11n (540 Mbps bandwidth)
Wireless Access Hardware	Ratio of 10-15 students or less per one access point/antenna in a classroom setting
	No structural walls or physical barriers between the access point and the students
	Wireless controller technology to enable access point load-balancing for optimum wireless access point utilization

The key design decision in any wireless network deployment is to determine which areas require coverage and what level of performance are required in those areas. The school environment introduces an additional challenge to the design considerations due to the structured nature of network use. For example, classes start at particular times and teachers often ask their entire class to start an activity at the same time. The structured nature of school network usage can greatly increase the peaks in load upon the wireless network. The general guidance for enterprise access point deployments has been 15 to 20 active clients per access point, but the peaks in demand at schools may require two access points per classroom, where there are 20 to 30 students in that classroom. The number of access points required per classroom depends on many factors, including the number of clients, the type of applications and the expected performance.

Note: All estimates in this document are dependent on ample bandwidth coming into the site and/or to the wireless access unit for distribution out to the instructional technology and/or testing devices.

Recommended Bandwidth Specifications	
External Connection to Internet	100 kbps per student or faster
Internal School Network	1000 kbps per student or faster

ADDITIONAL WIRELESS RECOMMENDATIONS

Develop and Maintain a Wireless Network Plan

Develop a wireless infrastructure plan that defines the strategy for either installing or upgrading your existing wireless network over the next three to five years. Elements such as wireless network security and the deployment, management and control aspects of deploying a wireless network must be included in the plan for successful implementation. This plan must be reviewed annually to keep it current with developing technologies.

Conduct a Physical Site Survey

As many educational institutions must contend with aging structures that contain enclosed classrooms, long hallways, remote and/or temporary buildings and construction materials that may prevent radio frequencies from smoothly passing through walls, it is recommended that a site survey of all instructional buildings in the district be conducted and reviewed annually. A site survey is useful for measuring radio frequencies coverage, which determines the locations in a school campus where the wireless network can be used. In addition to measuring coverage, the site survey is also useful for measuring the saturation point for the number of devices that can be used in a particular location. Both of these elements, coverage and saturation, must be considered as a part of the wireless network requirements.

Other site survey considerations are

Access Point Placement – In general, wireless access points must be located so that no obstructions exist between them and the students. When choosing the location of the wireless access point within the classroom, the Department of Education recommends the following:

- Locate the wireless access point in close proximity to the devices that will be connected;
- Place the device on a high shelf or mount it close to or on the ceiling;
- Ensure that the device is not situated near any metal objects, such as filing cabinets;
- Ensure the wireless antenna is in a vertical position;
- Ensure that you have conformed to the manufacturer’s guidelines; and
- Ensure there are no wireless access points in close proximity using the same or an overlapping channel.

Interference – Wi-Fi uses publicly designated radio bands to provide wireless access. Non-Wi-Fi devices like mobile and cordless phones, Bluetooth transmitters and security cameras may use the same radio bands and can interfere with and cause performance issues for a wireless network. Wi-Fi scanning tools cannot detect such interference; therefore, you will need to take these devices into consideration when conducting a site survey.

IEEE Standards

The Florida Department of Education’s minimum recommendation is the IEEE 802.11n equipment protocol standard that can handle radio signals in either 2.4 GHz range or 5 GHz range and bandwidth in the 540 Mbps range.

Consider the following when evaluating hardware devices.

- *GHz and Network Speed:* Higher GHz signals can carry more data than lower GHz signals; assuming that the electric power to the higher frequency radios is maintained at a higher level.

- *GHz and Network Range*: The higher the frequency of a wireless signal, the shorter the range and higher frequencies may not penetrate solid objects nearly as well as lower GHz signals.

- *GHz and Network Interference*: Lower GHz signals may pick up interference more than higher frequency GHz signals.

- *GHz and Network Security*: Higher GHz signals transmit data more securely over wireless Wide Area Networks (WANs).

When purchasing wireless networking hardware from separate vendors, make sure to obtain guarantees from the vendors that the hardware will interoperate with existing equipment and follow the IEEE standards. Older devices in the 802.11b/g/n standard can operate in the 2.4 GHz frequency band range. 802.11a/h/j/n standard devices can operate in the 5 GHz frequency band range. See Figure 1 for a list of IEEE 802.11 network protocols.

When evaluating the IEEE 802.11 standard with the computer devices that your school is using, consider the limits of the device itself in supporting the wireless access point standard that has been deployed. Also examine the demands of simultaneous users accessing online assessments or digital learning curriculum that may use video streaming and real-time learning tools.

Figure 1: IEEE 802.11 Network Protocols

802.11 Network Standards						
Protocol	Release Date	Freq.	Bandwidth	Maximum data rate per stream	Allowable MIMO streams (see School Wireless LAN Guidelines – Glossary)	Approximate indoor range
		(GHz)	(MHz)	(Mbit/s)		(Metres)
802.11a	Sep-99	5	20	54	1	35
		3.7				
802.11b (no longer in common use)	Sep-99	2.4	20	11	1	35
802.11g	Jun-03	2.4	20	54	1	38
802.11n	Oct-09	2.4/5	20	72.2	4	70
			40	150		70
802.11ac (DRAFT)	Draft released Nov-11	5	80	867	8	
			160	Between 1.73 Gbit/s and 6.93 Gbit/s		
802.11ad (DRAFT)	Feb-14	2.4/5/60		up to 7000		

Based on http://en.wikipedia.org/wiki/IEEE_802.11

Security and Access Management Policies
The Florida Department of Education recommends that each school implement the proper security protocols to secure and protect the information assets owned by the school. Appropriate security measures include network security monitoring tools, signal encryption, password authentication, firewall protection and virtual private network solutions.

All schools should have an active Acceptable Use Policy approved by their individual school board that includes a wireless communications section. Network filtering applications should be in place to comply with the Children's Internet Protection Act (CIPA).

At a minimum, the wireless communications section of the Acceptable Use Policy should address seven key areas that establish the basis for deployment, use and management of the wireless network.

1. ***Define the User Base***
   Identify who can use the Wireless Local Area Networking (WLAN) and what level of access each particular group of users will have on it.

2. ***Identify Appropriate Usage***
   Identify the type of information that users can and cannot send or receive over the wireless network. Prohibit users from sending personal information via the WLAN. Prohibit ad hoc connections such as peer-to-peer in order to avoid users having non-authorized access to your WLAN.

3. ***Prepare for Secure Installation***
   Identify which named individuals or internal departments are responsible for deploying wireless within the network. Define minimum physical security standards for Access Point (AP) locations, and determine who will have physical access to the Wireless Access Points (WAPs). Try to place your WAPs in controlled areas on interior walls of the school. Adjust their coverage zone to the limits of your physical boundaries and not beyond.

4. ***Establish Wireless Security Standards for the District***
   Define the minimum security measures enabled on all WAPs. Disable the service set identifier (SSID) broadcast feature and change the default SSID to something that does not reveal a school or district's name. Make sure that wireless authentication and encryption are enabled.

5. ***Outline Contingency Plan for Loss of Equipment***
   All security settings within the wireless network, including passwords and encryption keys, should be changed in the event of loss or stolen equipment. Best practices dictate to not store data on mobile devices and end-point security measures should be included. Treat any loss as a compromise to the system.

6. ***Plan Appropriate Training for Staff and Users***
   Outline minimum training requirements for all IT department staff and district users, and develop a knowledge base for proper WLAN use based on past successful implementations.

7. ***Establish Guidelines for Management and Monitoring***
   Purchase security monitoring software and define the frequency and scale of security assessments, which should occur on a regular basis to ensure continuity.

If implementing a Bring Your Own Device (BYOD) policy, make sure that Wireless Intrusion Prevention Systems (WIPS) are enabled to detect 'rogue' devices which are not part of your network.
Perform frequent security scanning to pinpoint any source of performance issues caused by interference between wireless access points and interference caused by other devices. Securing the WLAN is a continuous process implemented with regular monitoring.

School districts will need to allocate appropriate resources to manage the wireless network in the same manner as the wired network. A centralized monitoring, configuration, and reporting tool for the network infrastructure, such as a Network Management System or physical controller, is essential. This is especially true in situations where a school has more than two wireless access points servicing a classroom.

As with any network infrastructure, ensure that all wireless network infrastructure components meet or exceed manufactures' recommended environmental requirements in relation to acceptable humidity temperature and power conditions.