BYOD
(Bring Your Own Device)
Threat Vectors & Network Design

When considering BYOD remember that exploits can come from home or off site locations. The graphic notes devices that are mobile and have the ability to transfer exploits from off site locations into your school district. Mobile devices having this capability are noted with a ▼.

Threat Vectors

School Firewall

Local Switch

Servers/Workstations

School Wireless Network

Internet

Off Site Locations

Home

Public WiFi

Thumb Drives

CD/DVDs
There are many ways to design a secure BYOD solution. Below is one option using a wireless WiFi controller and a firewall.

The untrusted public wireless traffic is NOT allowed on the same network as the local school Lan and usually the only protocols allowed are http, https, and DNS. A policy MUST be configured in the firewall to deny public wireless traffic from entering the school Lan. (no hairpin traffic) If the firewall is capable, a rate shaping policy should be configured so that the public WiFi traffic will not consume all of the school's Internet connection.

Supporting notes are on page 3.
The wireless network solution for BYOD can be done in many different ways. The example above is one solution. Below are additional details supporting this example.

1. The Public WiFi and the Private WiFi are on two separate subnets. 192.168.1.0/23 and 172.16.1.0/24.

2. Having the public untrusted WiFi on it's own network allows for segmenting that network from the Private WiFi. It is very important to deny all Public WiFi traffic from entering the Private school network. Do the same denying local school traffic from seeing the public WiFi traffic. You don't want users bringing infected devices to school that could attack your local workstations and servers.

3. Firewall policies can be applied to the public WiFi that are separate from policies governing local private WiFi traffic. Some districts choose to only allow http, https, and DNS traffic on the public WiFi.

4. Using the PaloAlto Firewall as shown in the network diagram, you could apply Threat protection and content filtering to the public WiFi. The PaloAlto can also block specific applications like proxy, and those applications that are bandwidth intensive. A rate shaping policy can also be applied to the public WiFi only allowing that network to use a portion of the schools available bandwidth. This is critical; you don't want the public WiFi network to have the capability of consuming all of the school's bandwidth to the Internet.

5. The public WiFi, using the controller, can be configured with or without passwords. A Captive Portal can also be implemented stating school network usage policies (AUP) and asking for email addresses etc. when logging in. This is much like logging into a hotel WiFi. The Aruba controller in our network example has good firewall capability and can direct public WiFi traffic only to the Internet reducing the complexity of policies in the firewall.

6. VERY IMPORTANT - The outbound public WiFi IP address (NAT) should be different from the IP address used for local private school traffic. This will insure that, should there be an exploit residing on the public WiFi attacking IP addresses on the Internet the school's public IP address is not affected. (think about email blacklisting)

7. Passwords for the Private WiFi should NEVER be shared with anyone. The password for your Private WiFi should be changed often.

The comments above provide basic information about BYOD deployment. Deploying BYOD properly requires careful network planning and should be well thought out before implementation.