Bring Your Own Technology technical information

   LISD Technology has been working on the design for bring your own technology for almost a year. We began by having phone calls with other districts in the state that have been testing this to see what worked and did not work for them and to see how their security is handled. We learned some good tips from their experience. We also purchased consulting services from one of our trusted vendors, Resilient Intelligent Networks, to be sure we were secure and followed industry best practices for guest access. Resilient is a Master Elite Partner with HP for HP networking and wireless equipment. Resilient does a large amount of business for education and government customers. The BYOT was designed with security as the top concern. After various planning meetings and testing of options, we did the pilot at HHS 9th in the spring. The BYOT infrastructure was not hastily designed.

   BYOT uses a special wireless SSID called lisd-guest. This guest network uses secure guest access processes to create a secure wireless tunnel to the wireless controllers. One of our security concerns was how do we keep students from spreading viruses to each other since we have no control over their computers. The solution is that devices on the lisd-guest network are not able to see or communicate with each other at all so an infected computer cannot spread viruses. Another concern was how we keep a guest computer from infecting our main LISD network. The solution is that the lisd-guest traffic is tunneled externally to the internet and has no access to the main LISD network. All they can access are external addresses. This provides the guest network no access to our main network and any data stored there. These two features keep the student's devices isolated and keep back door attempts from being successful. When a student logs on to the lisd-guest network they have to use a web browser to access an encrypted authentication page were they are required to enter their active directory ID and password before getting on the guest network. All their traffic to the internet goes through our Telemate Netspective internet filter just like it would if they were on a LISD owned computer. This filter blocks inappropriate sites for students including social media sites. We also use a Juniper firewall for our core router that is top of the line equipment.