How do you protect students from themselves?

By Ellen Ullman

Last month we wrote about the evolution of one-to-one computing and how districts are allowing students to “bring your own device” (BYOD) to school. This month we look at how they are handling security and other issues so they can let students BYOD.

The Do-It-Yourself Approach

At New Canaan High School in Connecticut, students are welcome to bring in their own devices. “With the economy plummeting, this is the first time in my 28 years that we have more students in class than laptops on carts,” says Cathy Swan, technology integration specialist. “It’s great when a kid can supplement the cart.”

A student simply registers a device’s MAC address and the equipment is enabled for Internet access. Registration is simple: The Web site https://sites.google.com/a/ncps-k12.org/macaddress has detailed instructions for finding the MAC address, whether it’s a laptop, a smartphone, or an iPad. Students can fill out the form on a classroom desktop or on a computer in the library. Every week, the technology staff updates the list and adds the new devices to the network.

Since there is no school-wide mandate about BYOD, teachers have the flexibility to let students use their own devices or not; the tech staff merely makes it possible. “We’ve been doing this for a couple of years and have had zero problems since we started,” Swan says. “Students who have their own tech can use it; others use products that the school supplies.”

Network Segmentation

The Alvarado (Texas) Independent School District has been working on a one-to-one initiative since 2007. Today all students in the fourth through eighth grades have school-issued laptops. But because state funding has dwindled, the district has turned to BYOD.

Alvarado is already wireless, something Kyle Berger, executive director of technology, began working on before beginning the one-to-one program. He plans to segment the network and establish a quarantined network that will validate student devices after checking for updated antivirus tools and other requirements. “Basically, it’s like turning the school’s network into what you’d find at a hotel,” Berger says. “Students will open their device and get a screen asking, ‘Do you want to connect?’”

Berger feels comfortable with the technical aspects of BYOD but is less sure about how to handle the changes that will make instruction possible. He’s concerned about teachers having to provide lessons for a mixed
population of products. How do you teach about Excel spreadsheets, for instance, if one student has a two-inch screen and another has a laptop?

To address this matter, Berger’s team is working with a couple of vendors to deliver applications that will be device independent. “A lot of programs and resources are Web based or going up to the cloud, but on a small device the Web can be a problem,” he says. “For instance, iPhones don’t have Flash. We have to know that kids will get the content.”

Making a Public, Filtered Wi-Fi

Over at the Katy (Texas) ISD, content is not a concern, because the district has been preparing for BYOD in a number of ways. Two years ago, when the tech staff handed out mobile phones to fifth graders for a pilot project, they saw incredible instructional results, says Lenny Schad, chief information officer. Security was a nonissue, because Schad created a public Wi-Fi at the elementary school that was filtered in the same way the wired network was.

The Katy ISD has now distributed 1,500 mobile -learning devices to all the fifth graders at its 11 elementary campuses, and there is public Wi-Fi on 12 campuses.

When the children take their schoolsupplied mobile devices home, they connect to the Verizon network. These devices can connect to only that network or the Katy Wi-Fi network. Both networks filter Internet access through the district’s filtering system, which protects students from going to inappropriate Web sites.

This two-year program has laid the foundation for next year, when every campus will have a filtered public Wi-Fi and the district will allow kids to BYOD to school. In terms of curriculum, the Katy ISD has focused for the past couple of years on helping teachers integrate Web 2.0 tools into the curriculum; already most are comfortable teaching this way. “It’s an important thing people need to realize,” Schad says. “If you haven’t prepared your teachers for what to do [when you start a BYOD program], you won’t get your bang for the buck.”

Schad took a simple approach to security because he knew that teachers would need Internet access to use 2.0 tools. In keeping with that philosophy, teachers help students, even the youngest elementary kids, take digital responsibility and become smart and informed digital citizens. “We allow them to take advantage of Web 2.0 tools to collaborate, do their homework, and so on,” Schad says. “Otherwise, there’s no need for BYOD. The public Wi-Fi is just a continuation of a lot of things we’re doing. It’s a natural progression in this change cycle.”

A final, and perhaps the most important, reason the district is so keen on using Web 2.0 tools is that they are device neutral, and so another potential burden is removed. “Don’t want to add to a teacher’s overloaded workload,” Schad says. “Taking device specifics out of the equation makes it so much easier.”

Two Networks

Eric Willard, chief technology officer of Community Unit School District (CUS D) 300 in Carpentersville, Illinois, started his BYOD program by going through all the district’s policies and reworking the pieces that dealt with technology. He eliminated anything that stopped him from moving toward Web 2.0. That process took an entire year.

He spent another year working on district-level administrative procedures. “Lots of our leadership was saying no; they think cell phones are a nuisance,” he says. So he changed the procedures to align with the new policies and present no roadblocks to BYOD.

In September, Willard began implementation, but he then learned that many of the schools had handbooks that prohibited students from bringing in cell phones. Rather than push, he chose to delay for a year and go to each of his 27 buildings. He’s now listening to their concerns, informing them of the benefits of BYOD, and removing
any lingering barriers. "That’s where we are now," he says. "I intend to be open next year, and it will be a nonissue."

While Willard goes from school to school, he’s doing pilots and working on infrastructure. He recently completed putting in basic wireless access in every building and is about to add more IP addresses and build bigger firewalls that will handle additional users.

Currently, if a teacher brings in her own computer, she receives a password with which she can log on to the guest network. "Once we get more access for the kids, we’ll set switches up," Willard says. "They will have a different network they can access automatically; it will go through our filter and have a limited bandwidth pipe that doesn’t interfere with what school-owned computers are using. It might be a slightly slower network, but it will balance out."

**The Right Building Blocks**

Regardless of how a district chooses to handle BYOD and security, a few key steps make the entire process go much more smoothly. Willard has dubbed these steps "Willard’s Pyramid," a not-too-subtle homage to Maslow’s hierarchy of needs. Here are the pieces of Willard’s Pyramid:

**Funding and leadership.** These crucial elements are the base of the pyramid, he says. "Without those in place, don’t bother going forward."

**Technology planning and support.** "Make sure all stakeholders are involved from the beginning. Figure out what you have and where you want to go. Build a team that supports what’s in place today or you won’t get the credibility to continue."

**Standards and infrastructure.** After the tech planning, it’s time to develop a series of standards, including hardware, software, instruction, networking, and infrastructure. "At this point you’ll know if you need fiber between buildings, and so on. Then you can start buying hardware and software."

*Ellen Ullman is editor of School CIO.*

Print this document