# Mobile Laptop Labs

Print this page

*by Cary Hellman, College Park High School, Pleasant Hill, California and Matt Hiefield, Sunset High School, Beaverton, Oregon*

**Other Recommended Hardware**

To maximize the value of a mobile laptop lab, you must be able to access networked resources, such as file servers and printers, and the Internet. Even though wireless networking technology has become standardized and affordable, it's recommended that each classroom have a "network drop" (two to four RJ-45 jacks) enabling wireless networks to interface with the school's Local Area Network (LAN).

This involves:

- Wireless network access point(s). There should be one for every 10-30 laptops (depending on brand and model), based on the IEEE 802.11 standard (strongly recommended), and with one PCM wireless network card per laptop.
- Laser printer (one per cart). This should be network-ready with a moderate usage capacity.
- Ethernet mini-hub and CAT5 patch cables (so you can provide connections for the access point and printer). The hub will need an uplink port to connect the wireless network to the school's LAN.
- Extension cords and power strips. Have a procedure in place to provide AC power to the laptops for the times when batteries run down.

**Security Issues**

Security of hardware, software, and data is paramount in ensuring the success of a mobile laptop program, especially one that may include a separate set of equipment available for student check-out. Here are a few of the major issues to consider:

**Hardware**

The biggest concern with hardware is the risk of vandalism and theft. Even an extended three-year warranty from the vendor will not suffice if an LCD screen is broken or equipment is stolen. One approach to addressing this risk is insurance, and there are policies designed specifically to meet the needs of schools.
Another approach to security is deterrence, including both supervision and active protective measures. For example, you can attach security anchors and cables to secure the access point and networked printer to the cart, although this approach is not advised when it comes to laptops. (It's not practical to expect teachers to cable laptops to each desk or table in the classroom; neither is it desirable if you want to take full advantage of mobile computing.)

As an alternative to anchors and cables, consider I.D. plates, alarm systems, or tracking-and-recovery software. You can permanently affix (to each laptop) a metal I.D. plate showing a unique bar code, an I.D. number, and the school's name. Alternatively, you can install alarm systems, which involve a transmitter mounted on the cart and a receiver mounted on each laptop. To protect against the rare case when even these deterrence systems might fail, you can install special tracking-and-recovery software on each laptop. Should a laptop be stolen, it can be tracked and recovered if the thief uses the stolen laptop to access the Internet.

For more information on these devices and technologies:

- Alarm systems (TrackIT)*
- Anchors (SPOT)*
- I.D. plates (STOP)*
- Insurance (Safeware)*
- Tracking-and-recovery software (CompuTrace)*