WHITE PAPER

CDW·G PEOPLE WHO GET IT

BRING YOUR OWN DEVICE

Adapting to the flood of personal mobile computing devices accessing campus networks

Executive Summary

The "bring your own device" (BYOD) movement is relatively new in corporate and K–12 environments, but colleges and universities have been adapting their networks and policies to accommodate personal mobile computing devices for quite some time. Undergraduate and graduate students have been bringing their own wireless-enabled notebook computers and smartphones to campus since the dawn of the 21st century. What has changed in recent years is the quantity of mobile devices that these students now carry and the fact that so many of them expect their institutions to provide ubiquitous, reliable wireless connectivity.

These days, many students, faculty and staff members arrive on campus with a notebook computer, smartphone, an MP3 player and sometimes a tablet, e-reader or other IP-connected gadget. And they presume that they will be able to use any and all of these personal devices to access the network and its resources in real time, from anywhere.

Colleges and universities are struggling to meet these expectations. One reason is that administrative priorities often are at odds with this rapidly evolving culture of 24x7 access. According to CDW·G's 2011 *21st Century Campus Report*, 22 percent of administrators cited the use of technology to enhance student learning as one of their top two priorities for the 2011–2012 academic year; a mere 12 percent said the same about improving and enhancing IT.

Within the constraints of tight budgets, higher education leaders are now rethinking their IT strategies in order to meet these expectations of anytime, anywhere access and technology-enhanced learning. Many institutions need to upgrade their network capacity and performance by increasing bandwidth, adding access points, boosting their network management capabilities and addressing security concerns. They also must make core applications and

TWEET THIS!

Table of Contents

resources available to students, faculty and staff via mobile devices and ramp up efforts to implement virtualization and cloud computing technologies.

Institutions that are proactive in their response stand to gain critical benefits. If faculty can more fully integrate technology into their curricula, they'll see improvements in student participation, collaboration and learning outcomes. A robust mobile-enabled environment also can be a powerful competitive differentiator in a college or university's efforts to recruit top students.

Why Support Pervasive BYOD?

Postsecondary students once looked to academic departments for recommendations on which computing products to purchase and bring to class. But today's generation of college students is far more technologically savvy. They tend to use their own mobile computing devices daily in both their personal and academic lives. Indeed, Student Monitor, a provider of college student–centric market research services, found that 88 percent of students access the web every day to do research, engage in social networking, check e-mail, text friends, collaborate or create content.

Not surprisingly, this consumerization of technology has helped fuel the use of mobile devices on college and university campuses. At the University of Tennessee, Knoxville, for example, 27,500 students and 9,700 faculty and staff members have registered 75,000 devices for use on the university's wireless network, which averages out to 2.1 devices per user. (Some institutions have reported device-to-student ratios as high as 3.5-to-1.)

Doyle Friskney, chief technology officer at the University of Kentucky, believes this student-driven model has become so infused in the campus culture that it's become impossible to institutionally direct and control. Indeed, in many ways, students are now setting the IT agenda. Although the implications of this new reality for campuses are still unfolding, those that don't quickly adapt are likely to see their ability to compete for the best students weaken.

Students increasingly see technology as paramount to their academic success, and they expect colleges and universities to support their technology needs and expectations. According to the *21st Century Campus Report*, 87 percent of current college students considered technology offerings when deciding which institution to attend. And 92 percent of current high school students said that technology will be a key differentiator during their university selection process.

And it's not just because they prefer using their own devices. A BYOD environment that's well-supported by institutions — and integrated into their current long-term academic and technology strategies — offers several key advantages to students:

- **ENABLES TECHNOLOGY-RICH CLASSROOMS:** The *21st Century Campus Report* found that technology is slowly being adopted into college and university curricula. Notably, 31 percent of students used technology as a learning tool while in class in 2011 (up from 19 percent in 2010).

  Pervasive BYOD will help foster this trend, as faculty will be able to assume that most students have access to mobile computing devices and have confidence that the requisite wireless bandwidth is available to support them.

- **INITIATES NEW WAYS OF LEARNING:** According to Lee Rainie, director of the Pew Research Center's Internet & American Life Project, mobility and wireless connectivity are creating new kinds of learners who are more self-directed in their acquisition and sharing of knowledge, more inclined to collaborate and more reliant on feedback.

- **INCREASES STUDENT ENGAGEMENT:** Students who use their own personal devices for anytime, anywhere access will engage more in classroom activities, collaborate more fully with classmates, communicate with faculty and learn how to solve problems using the latest skills.

Mobile Applications

The support burden will intensify as bring your own device (BYOD) becomes increasingly omnipresent on college and university campuses. A student might access a course management system from a notebook computer while studying in the library one day, for example, and then use a smartphone the next day to register for classes or check a financial aid application.

To accommodate this expectation of easy access from any device, schools must "mobile-enable" their institutional resources to work with various types of operating systems and hardware platforms. Campuses are moving forward, but progress is slow, says Dr. Susan Grajek, vice president for data, research and analytics at the EDUCAUSE Center for Applied Research (ECAR).

ECAR's *Mobile IT in Higher Education, 2011* report found that a few institutions have "mobile-enabled" some campus services (particularly those that meet student or public needs), but 38 percent have made no progress in this area. Campuses that have created mobile applications are focusing their efforts in specific areas.

MOBILE APP FOCUS	
Primary website	**40%**
Learning/course management system	**38%**
Library catalog and other library services	**31%**
Student recruitment and admissions	**23%**
Administrative services for student information	**22%**

TWEET THIS!

Preparing the Network

Providing sufficient bandwidth is the biggest BYOD-related network challenge that campus IT leaders face. As mobile learning devices are integrated into the curricula and campus life, users who have come to think that 24x7 wireless connectivity is a right and not a privilege will have zero tolerance for a network that slows markedly during peak usage or becomes unavailable to them, according to Kenneth C. Green, founding director of The Campus Computing Project.

Fortunately, higher education institutions have a strong foundation upon which to build. The *21st Century Campus Report* found, in fact, that 85 percent of colleges and universities already provide wireless network/Internet access and 72 percent offer remote access to their networks.

However, planning for bandwidth needs should take into account more than just the proliferation of mobile devices. Today's students regularly engage in bandwidth-intensive activities (including social networking, video-on-demand, video streaming and multimedia) to meet both academic and personal needs.

As Raechelle Clemmons, chief information officer for Menlo College, has noted, the notion that "if you build it, they will come" perfectly applies to wireless networks. The more bandwidth an institution makes available, the more users will take advantage of it.

If the wireless access is robust enough, users who have traditionally relied on the wired network to access resources will likely switch to wireless. They also could potentially turn to the campus wireless network for decidedly nonacademic purposes (to watch a movie online during a break between classes, for example).

For this reason, institutions looking to support pervasive BYOD must upgrade their network backbone, add more and better wireless access points to provide dense coverage throughout the campus and adopt a unified threat management (UTM) approach to securing network transmissions.

Campus IT leaders also should consider the following strategies to ease the burden of more mobile devices accessing the network:

- **PRACTICE INTELLIGENT WIRELESS MANAGEMENT.** New advanced management consoles can help institutions proactively manage limited bandwidth by providing a universal view of all devices and access points on the network. These tools also enable the labeling and prioritizing of traffic to better balance the load during peak usage.
- **RETHINK COVERAGE.** Colleges and universities used to concentrate access points in classrooms, libraries, dormitories and other campus hotspots where students congregated to study and socialize. But the ubiquity of mobile devices (especially smartphones) in students' lives demands anytime, anywhere network connectivity, including in hallways, on bike paths, and in athletic facilities and special-event venues.
- **PLAN FOR GROWTH.** Any investment in wireless technologies should support a modular approach, says Philippe Hanset, network architect for UT Knoxville. Demand for network performance and access will increase exponentially, and campuses must be prepared to add resources as needed.

Are Computer Labs Outdated?

Computer labs have long been essential to college and university life. Despite the pervasiveness of personal computing devices on campus, computer labs are still surprisingly popular with students, says Kenneth C. Green, founding director of The Campus Computing Project.

Several factors ensure that computer labs will remain campus mainstays for the foreseeable future:

- **The Digital Divide:** The price of most mobile devices is fairly low, but not all students have the financial resources to buy the latest-and-greatest gadgets. Some students still come to campus with older computers that don't have the processing power or graphics cards necessary to run newer applications. Others can afford only low-end computers or invest instead in smartphones or tablets. These students will need access to computer labs for certain core functions (such as printing), so campuses will need to provide them.
- **High-end computing:** Students in technical fields of study, such as mathematics, engineering, architecture and finance, may not be able to afford the specialized applications that their classes require them to use. In most cases, academic departments provide access to these programs in computer labs.
- **Convenience:** The fact remains that many students like to hang out in computer labs, sometimes for social or collaborative purposes and sometimes because they simply want to work on computers that have more, better or different features than their own.

Addressing Security Concerns

Because BYOD isn't new, colleges and universities already have established role-based authentication and virtual local area networks (VLANs) that prevent students from accessing internal applications, databases and other sensitive or confidential data. Of greater concern is the possibility that personal devices carrying viruses will reach the network and potentially infect internal campus resources.

Higher education institutions are taking different approaches to securing their networks within a BYOD environment. Among the steps being taken, campus IT leaders are:

- **Requiring users to register every device** (including gaming consoles), so that if a virus is introduced or a device attempts to access inappropriate areas, IT staff will have a way to tie devices to their users
- **Utilizing two-factor authentication,** in which both the user and the device are verified before network entry is allowed
- **Providing antivirus and antimalware software** for all student, faculty and staff computing devices
- **Scanning devices at their points of entry** to ensure they have virus protection and required patches
- **Educating students, faculty and staff** about security practices and network policies, as well as their own responsibilities as users, before network privileges are granted
- **Verifying users' understanding** of these practices and policies via signature or timestamp
- **Locking down the core network** by adding additional firewalls around university financial systems and other mission-critical applications or databases
- **Relying on virtualization and internal clouds** to further protect financial and personal data

Best Practices

The rapid expansion of BYOD complements other trends taking place in higher education, including virtualization and technology-enhanced classrooms. The following best practices can help campuses adapt even more quickly.

SECURE FACULTY SUPPORT. According to the *21st Century Campus Report*, the No. 1 challenge campuses face in their efforts to increase classroom technology use is the faculty's lack of technology knowledge. And although 81 percent of colleges and universities are providing technology-specific professional development, faculty members said that the most used approaches (group meetings and seminars, videos and online tutorials, one-on-one meetings and peer mentoring) are missing the mark.

Professional development sessions would be more effective, they added, if the people who actually use the technology in the classroom led the training and if the sessions were targeted to the unique needs of specific academic disciplines.

DEPLOY VIRTUALIZATION. BYOD and virtualization are sister concepts in that they both enable anytime, anywhere computing via the web. Campuses can streamline their efforts to support both the BYOD revolution and the diverse computing needs of students, faculty and staff by virtualizing servers, clients, applications and storage. This allows users with outdated notebooks to perform the same tasks as those with more cutting-edge technology.

Last year, Menlo College's IT department made virtualized clients available to students enrolled in a financial accounting class. The move gave students 24x7 access to classroom assignments and notes and allowed them to work in specialized accounting software applications, store their in-progress projects and collaborate with other students.

Virtualization also can help colleges and universities lower computing and labor costs, increase flexibility, improve security and reduce their carbon footprint.

RETHINK SUPPORT POLICIES. BYOD takes a lot of pressure off of the IT department because students, faculty and staff are responsible for fixing or replacing their malfunctioning or damaged personal devices.

However, IT personnel must help these users access the network. And with the variety of operating systems and platforms that students, faculty and staff are bringing to campus, that can be a tricky endeavor. The best way to overcome this challenge is to develop written policies that specify which platforms the IT department will support.

CDW·G's Mobility Solutions

CDW·G offers services to support BYOD on college campuses:

Procurement and activation: CDW·G is an authorized partner with AT&T, Sprint and T-Mobile for the procurement and activation of devices. Through strategic partnerships, CDW·G can also activate selected devices with Verizon Wireless.

Securing and managing devices: CDW·G can provide multi-OS device security and management software including BlackBerry, iOS, Android, Windows Mobile, Symbian Device Security and Management. Partners include AirWatch, BoxTone, McAfee, MobileIron, RIM, Sybase and Symantec.

Supporting mobile solutions: CDW·G can help with building customized procurement portals, creating IT help desk Tier II and III support solutions, charge allocation and reporting, end user support, bill auditing, management and reconciliation, and asset tracking and inventory management.

Learn more about CDW·G's offerings and hear a mobile deployment story from one of CDW·G's wireless solution architects at CDWG.com/mobility – or contact your account manager.

TWEET THIS!

CDW·G PEOPLE WHO GET IT