Transforming higher education with mobility solutions

A strategic guide for colleges and universities considering bring-your-own-device support models

Kathy Karpinski, Dell Inc.

Table of Contents

Change is here 3

What is BYOD? 3

Why consider BYOD programs now? 4

Challenges posed by BYOD 4

Benefits of BYOD program adoption 5

Dell can help 7

Define policies for devices 7

Protect your data 7

Empower your students with access to data anytime and anywhere 8

Dell offers a broad selection of mobility solutions 8

Device management 9

Secure data from the device to the data center 9

Solutions for developing and modernizing applications 10

Optimizing infrastructure to meet the challenges of mobility 10

Endpoint devices with consumer appeal 10

Transforming your university 10

Transforming higher education with mobility solutions

A strategic guide for colleges and universities considering bring-your-own-device support models

Change is here

Over the past decade, technology has radically transformed the higher education experience. Learning has moved out of the classroom, with students expecting that they'll be able to pursue their education from any location at any time. According to the National Center for Education Statistics, 20 percent of undergraduates and 22 percent of postbaccalaureate students attended at least one distance learning class in 2008 (the most recent year for which data is available).[1] In addition, 4 percent of all undergraduates and 9 percent of master's and doctoral students took only online classes. And those percentages have undoubtedly risen since.

Five years ago, students generally accessed distance learning classes via their laptops or desktops, but that model is also changing as increasing numbers of students use smartphones and tablets to access the Web.

Today, students, faculty, staff and even administrators want to access organizational resources via their mobile devices. According to the Center for Digital Education, 78 percent of students and 83 percent of faculty and staff are bringing a personal device to class and using the campus network.[2]

For higher education IT departments, bring your own device (BYOD) is already a reality, whether or not they have specific BYOD policies in place.

What is BYOD?

In higher education, IT support models are changing. Whether you support a multicampus state university, a small liberal arts college, a community college or a for-profit educational institution, innovative technology has fundamentally changed how people work, teach, learn and interact. Gone are the days when students did most of their work in a school-run computing lab. Today, students and faculty expect to be able to access school systems from anywhere, at any time, via any device they choose.

In some ways, colleges and universities are better prepared to deal with the BYOD trend than other organizations and corporations. After all, students have been bringing their own desktops and laptops to campus for decades. What's changing is that students, faculty and staff are increasingly using smartphones and tablets for tasks that used to be done with PCs, and they're accessing resources and services through apps. IT departments face the task of supporting new platforms, as well as the management difficulties that arise when faculty and staff use devices that they personally own instead of rely-

[1] http://nces.ed.gov/fastfacts/display.asp?id=80
[2] https://www3.gotomeeting.com/register/553133214

ing on hardware provided by the college or university.

The BYOD era presents new challenges and opportunities for colleges and universities. The ability to offer device choice without sacrificing control or increasing security risks becomes the new measure of success for higher education IT organizations. BYOD presents an opportunity for college and university IT departments to reevaluate and **transform basic IT principles** of how to support their users with long-term benefits for growth and scale.

> “[BYOD] has altered the way we protect the institution tremendously because we have to allow more openness. ... We have to move forward and realize there is a revolution in IT.”[3]
>
> George Baroudi,
> CIO, Long Island University

Why consider BYOD programs now?

IT departments are under constant pressure to do more with less — to deliver more technology with fewer resources, tighter budgets and less time. In an era when technology is evolving at a rapid pace, traditional models of support are tested to the limit and often found inadequate to meet the organization's increasing expectations. When implemented with the correct strategy, technology and training, BYOD support models can positively redefine the role of IT, improving the delivery of education and improving faculty, student and staff satisfaction.

Many organizations embark on the path of BYOD based on pressure from their users, who simply want to utilize the same devices and technologies in the college or university setting as at home. This pressure significantly increases the number of personally owned devices projected to enter higher education IT environments over the next several years. According to ECAR, 62 percent of undergraduates owned a smartphone in 2012, up from 55 percent in 2011. More significantly, the number of students who said they used their smartphones for academic purposes nearly doubled between 2011 and 2012.[4]

Support of a BYOD model represents a fundamental shift in IT management philosophy, as considerations must be made for end-user behaviors, remote support and, potentially, the virtual delivery of applications onto a spectrum of dynamically evolving mobile devices. As organizations begin migrating from older operating systems to Windows 7 or Windows 8, that migration often provides a prime opportunity to rethink the role of IT and implement new support models.

Several factors are shaping the BYOD landscape:

- Blended learning environments supporting online learning and massive, online, open classes (MOOCs) are placing new bandwidth and scalability demands on existing network infrastructure. Educational institutions can inspire collaboration and foster more opportunities for learning and scholarship by providing access to institutional resources anytime, anywhere, from any device.
- IT leaders are looking for ways to automate and improve IT processes.
- New IT configurations are needed to deliver seamless, delightful end-user experiences to students and faculty accessing university classes, applications and data remotely and from multiple devices.
- IT managers have security concerns when students access university data, sites and applications from personal devices.

Challenges posed by BYOD

BYOD poses considerable IT complexity and risk for institutions that idly stand by. The following challenges must be taken into consideration when crafting a BYOD strategy:

Increased security risks. Many smartphones and tablets are not built with security features and do not come with the support services necessary for university use. In fact, “four in 10 mobile users will click an unsafe link while using their smartphone this year, according to Lookout Security. Yet less than a fifth of consumer devices run any antivirus software, according to security research organization SANS.”[5] Increased virus, malware and hacker attacks become a reality when students, faculty and staff access the network, applications and data with devices outside of IT governance and control.

[3] http://www.informationweek.com/hardware/handheld/ipad-university-it-lessons-from-college/240010025

[4] Eden Dahlstrom, with foreword by Charles Dziuban and J. D. Walker, ECAR Study of Undergraduate Students and Information Technology, 2012, Research Report (Louisville, CO: EDUCAUSE Center for Applied Research, September 2012); available from http://www.educause.edu/ecar

Data protection and device loss prevention. BYOD requires encryption features and the ability to store data centrally in the data center and not on the endpoint. Loss and theft of smartphones, tablets and PCs when faculty and students are on the go is a real threat to data security that must be planned for and mitigated when implementing a BYOD program. 60 million smartphones are lost, stolen or damaged each year,[6] and more than two million laptop computers are stolen, lost or misplaced in the U.S. annually. Laptop theft has been growing at a steady rate; one in 10 laptops will be stolen within its lifetime.[7]

Maintaining bandwidth and uptime requirements. Network bandwidth and storage can become expensive and difficult to maintain in a university or higher education environment. Students, faculty and staff may want to access your environment with multiple devices. How do you keep your systems from crashing when thousands, not hundreds, of students attend an online class or webinar? Can your environment scale? Long Island University ran into this problem when it instituted a BYOD program that involved giving each incoming freshman a free tablet. According to CIO George Baroudi, network demand quadrupled in the first year after the program began. Although the university originally set aside $160,000 for network infrastructure upgrades, it finds that it must now set aside the same amount of money every year to continue improving capacity.[8]

IT complexity. IT departments in academia are often resource constrained. Maintaining an environment that's accessed by multiple device types and different operating systems, all outside IT control, as well as providing some university-owned clients, devices and workstations for libraries, group study areas or high-tech labs, increases IT complexity. In addition, creating and pushing mobile university apps to multiple device types may require skills beyond that of some higher education IT departments.

HR implications. When the same device is shared for personal and work use, faculty and staff may access websites, send photos or engage in online interactions that normally are not allowed. Institutions must rethink their HR policies and enforcement on endpoint devices when implementing BYOD programs.

Despite the complexity of BYOD, institutions should realize that ultimately, today's academic workforce and student base are evolving, and to stay competitive, they not only must appeal to new trends, but also provide them with the tools, apps and access that improve productivity and satisfaction, and that best enable their them to do their jobs efficiently and effectively.

Benefits of BYOD program adoption

Several factors are driving consideration of a BYOD strategy beyond student and faculty demand. Adopting BYOD provides benefits across your institution. BYOD programs can help create a learning environment that is evolved, more engaged, more connected, aware and more agile.

BYOD programs enable a seamless workplace for faculty and staff, regardless of whether they are in a classroom, in their offices, working from home or traveling. Anytime, anywhere, any device access makes it possible to receive and

[5] David Goldman, “Your Smartphone will (eventually) be Hacked,” CNN MoneyTech, September 17, 2012. http://money.cnn.com/2012/09/17/technology/smartphone-cyberattack/index.html

[6] Henry, Veronica. “How to Find Your Lost or Stolen Device”, August 17, 2012 via ReadWriteMobile.com.http://readwrite.com/2012/08/17/the-best-ways-to-find-your-stolen-mobile-device

[7] The Billion Dollar Lost-Laptop Study” survey conducted by Intel Corporation and the Ponemon Institute, 2010.

[8] http://www.informationweek.com/hardware/handheld/ipad-university-it-lessons-from-college/240010025

respond to internal communications almost immediately. Just as important, faculty members interacting with students are able to significantly improve their response and communication, thereby improving the educational experience. And prospective students will likely be drawn to colleges and universities that allow them to access networks from their choice of devices.

At an organizational level, IT should assess four key areas when planning and implementing a BYOD strategy: management of mobile devices and data; data security; application development and modernization; and infrastructure optimization. BYOD programs and solutions can lead to significant benefits realized in improved efficiency, increased user productivity, and reduced operating costs — all of which set the course for transformation.

Mobile device management. Today, IT is challenged with evaluating alternative forms of management for smartphones and many non-Windows tablets. Traditional management suites are not designed to keep up with the dynamic evolvement of today's mobile products. For that reason, mobile device management (MDM) tools are critically important. MDM allows IT to automate and centrally manage a heterogeneous mobile device environment through enforcement of organizational policy. The MDM tools offer user flexibility without IT intrusion.

Data security. As a cornerstone to BYOD justification, desktop virtualization technologies allow IT to remotely and securely manage the flow of data on devices. Data no longer resides on the physical device; rather, it is centrally managed by IT in a host of different locations that may include an on-premises data center or a private cloud service. By using virtualization technologies along with secure networks and mobile device management tools, IT can enable a more mobile, flexible and productive BYOD environment while confidently protecting sensitive data at rest or in motion, regardless of the brand of device or version of operating system.

Application development and modernization. Mobile applications facilitate an environment that allows faculty, staff and students to work at any time, on any device and from any location. Analyst recommendations support the premise that organizations should continue to invest in the development of new applications as well as the modernization of existing applications. Although complex on the surface, the modernization of applications is critical for the long-term success of a BYOD initiative. With fewer resources to operate and maintain older, legacy applications, this process becomes an important decision for any organization considering a BYOD program. It typically consists of application rationalization, re-hosting considerations, and potentially code migration to ensure compatibility and seamless delivery onto any device, regardless of the display size or version of operating system. The ability to leverage the advanced capabilities of new smart devices, improve application performance, and enhance overall usability ensures that organizations remain competitive while at the same time avoiding unnecessary costs with maintenance and support of legacy applications on aging, obsolete devices. Some institutions may decide to undertake these tasks on their own, while others may elect to engage experienced professional services organizations for assistance.

Infrastructure optimization. Influenced by the technologies and driven by users, BYOD stretches the limits of innovation for most organizations. The introduction of BYOD into the mix encourages administrators and IT leaders to openly consider changes to technologies and processes leveraged in the data center or through cloud service providers to optimize the virtual delivery of applications used by employees on their personal devices. With the convergence of servers, storage, network and the cloud through unified policy-based tools, IT can automate routine administrative tasks that allow IT to focus on its core functions. For example, network administrators can focus on tasks such as WAN optimization, firewall security, and throughput. Storage administrators can focus on storage functions, which include load balancing. All of these are critical to the optimal delivery of a secure environment on mobile devices.

Dell can help

When thinking about your university's approach to BYOD, it may be best to consider all of your mobile technology devices and plan for a full mobility transformation. Implementation of a mobility program will test the creativity and capabilities of most IT organizations. Dell is uniquely able to help you assess, define and implement a mobility program tailored to your unique needs and challenges. Dell has a strategic approach for enabling your institution to implement the most comprehensive spectrum of mobility solutions that enable seamless, dynamic, anytime, anywhere access to your organization without sacrificing IT control.

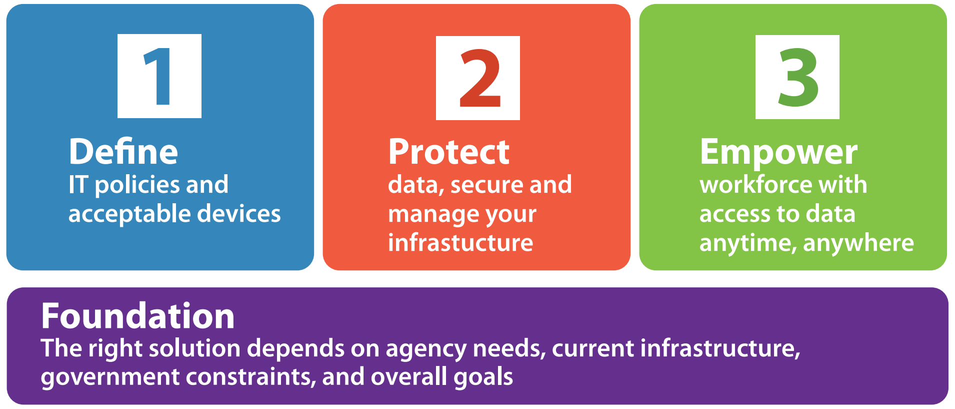
Dell recommends a three-step approach to mobility transformation, starting with an organizational evaluation.

The foundation on which you roll out a mobility program depends largely on characteristics of your institution. Many vendors offer mobility solutions built to solve a technology problem. However, the successful mobility strategy starts with an evaluation of your institution(s), its culture, risk tolerance, your current IT environment and goals, and the characteristics of your faculty, staff and students. You must consider your infrastructure's ability to scale with increased network traffic or data storage needs, for example.

Define policies for devices

Once you understand your organization's foundation, begin to define policies and determine acceptable devices. Success requires you to understand and segment your end users by role and by technology and access needs.

Three key elements to enable the evolving learning environment



1 **Define** IT policies and acceptable devices

2 **Protect** data, secure and manage your infrastucture

3 **Empower** workforce with access to data anytime, anywhere

Foundation The right solution depends on agency needs, current infrastructure, government constraints, and overall goals

Review existing policies and/or create new policies for areas such as:

- Device access
- Approved devices
- Usage policies
- Security policies
- End-user support

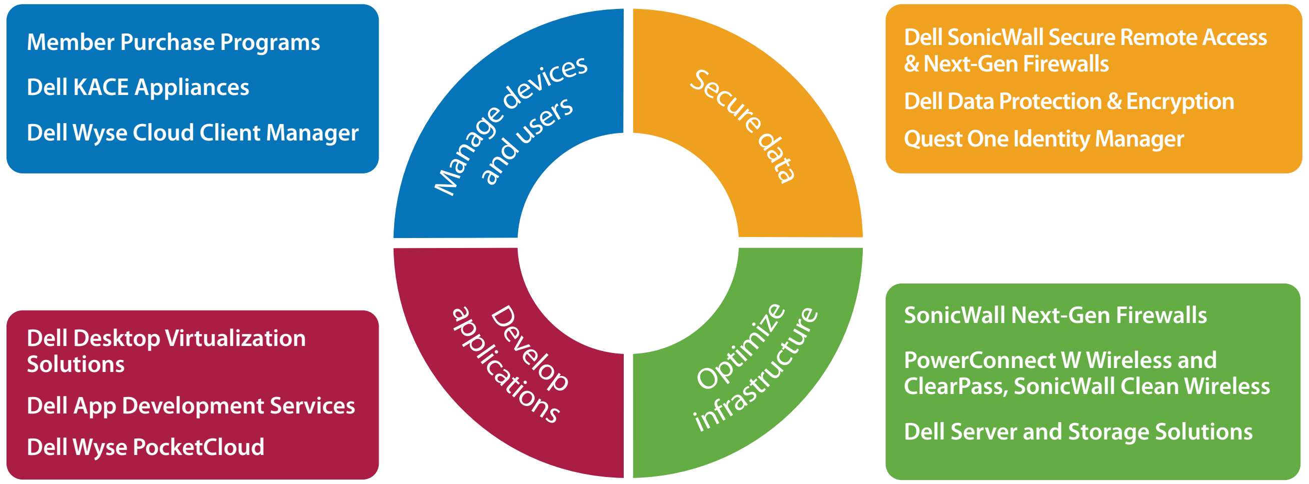
Mobility solutions require a new commitment, understanding and relationship among staff, faculty, students and data. Working with a trusted partner such as Dell can help simplify the process of determining policies for BYOD. Policy creation should be prioritized and enforced.

Protect your data

Dell recommends an end-to-end, holistic approach to security. Update your security strategy and use technology that protects IP and data on the device, the

Dell offers a broad set of solutions to enable mobility

Allowing access to corporate email, apps and desktop on smartphones, tablets and PCs



Member Purchase Programs
Dell KACE Appliances
Dell Wyse Cloud Client Manager

Dell SonicWall Secure Remote Access & Next-Gen Firewalls
Dell Data Protection & Encryption
Quest One Identity Manager

Dell Desktop Virtualization Solutions
Dell App Development Services
Dell Wyse PocketCloud

SonicWall Next-Gen Firewalls
PowerConnect W Wireless and ClearPass, SonicWall Clean Wireless
Dell Server and Storage Solutions

network and in the data center; your data must be secure while at rest and in transit. A modern converged information security approach enables access to information outside the physical network, including mobile, social and cloud hosted applications, by dissolving the perimeter.

Dell recommends a four-step approach to security:

1. **Embed** security into devices and platforms with integrated security.
2. **Protect** your data from device to cloud through data encryption, data and server backup and recovery, virtual private network (VPN), next-gen firewall and application control, identity and access management, desktop virtualization, patch management, and performance and availability management.
3. **Be able** to proactively see and stop risks before they affect your environment through threat intelligence, audit and assessments.
4. **Respond** immediately to an information breach.

Also consider deploying cloud client computing solutions that include desktop virtualization and thin/zero clients so that data is never physically on the device.

Mobility solutions provide an opportunity to strengthen your security and take advantage of the latest security technology.

Empower your students with access to data anytime and anywhere

The first step in empowering your organization is thinking through your application strategy. The four most popular applications that end users are looking for are email, Microsoft applications, file servers and VPN. You'll need to determine the best method to enable access to these applications. Implementing centralized, automated systems for endpoint and mobile device management can also greatly improve IT productivity. In addition, moving desktop life-cycle tasks to the cloud through desktop virtualization or solutions delivered as a service or through fully managed options makes better use of IT resources.

Dell offers a broad selection of mobility solutions

Unlike the competition, Dell is the only IT solutions provider offering a complete spectrum of mobility solutions that enable you to manage all the devices in your environment, protect data from the edge to the data center, develop and deliver apps for improved end-user productivity and optimize your infrastructure for a dynamic, seamless end-user experience.

Dell mobility solutions address four major areas of concern for organizations:

Device management

Dell has multiple solutions for mobile device management. Dell Cloud Client Manager is a SaaS solution that enables inventory management, group policy creation and device monitoring. In addition to iOS and Android mobility devices, Dell Cloud Client Manager also enables you to manage thin clients and remote desktops — functionality not available from the most popular MDM providers.

KACE K3000 is an appliance that offers MDM and mobile application management (MAM) capabilities, including inventory management, device, application and profile management, mobile device security, group policy creation and device monitoring, to name a few, for customers who prefer an on-premises management solution. KACE K1000, K2000 and K3000 provide automated and simplified management and deployment of all endpoints including PCs, servers and mobile devices.

Dell Desktop Virtualization Solution (DVS), a component of Dell Cloud Client Computing solution, provides IT decision makers with the ability to push a virtual desktop to any personal PC or Mac without exposing any data to the hard drive. This solution gives the end users a dynamic, seamless experience by providing access to the applications they need while preserving the privacy they require on their personal machine. End users will not experience bandwidth issues and will enjoy connectivity from any location, at any time and on the device of their choice — improving productivity.

Secure data from the device to the data center

Dell provides complete, connected security solutions. Dell SonicWall SSL VPNs provide industry-leading, secure encrypted tunnels from the device to your network. Dell SonicWall solutions enable authentication and access control regardless of device type. In addition, Dell SonicWALL Next-Generation FireWall is ranked No. 1 by NSS Labs for overall projection and value.[9] These firewalls provide deep packet inspection and real-time monitoring to keep the network safe. Dell Data Protection and Encryption (DDP|E) enables data encryption while data is at rest on a PC, on a mobile device or in the cloud. In addition, Dell Quest One Identity Manager provides an enterprise-wide solution that streamlines the access governance process of managing user identities, privileges and security. Dell Quest Webthority provides secures remote employee access to applications and systems, based on established policy, infrastructure, and authentication and authorization practices. And Dell Latitude 10 tablet, Dell XPS 10 and XPS 12, and Precision workstations are all built with enterprise-class features and encryption and security, Dell award-winning ProSupport that keeps your data

[9] 2012 Next-Generation Firewall Security Value Map™, NSS Labs, Inc., 2012

safe on the device — in an attractive, sleek, consumerized design.

Solutions for developing and modernizing applications

Dell Application Development Services can define, develop, test and deploy applications to work on devices such as smartphones and tablets.

Dell Quest vWorkspace and vWorkspace – MokaFive Suite offer a Web access portal that gives corporations the tools needed to create app stores and portals for virtual and offline desktops, providing a system for effectively delivering applications in virtual environments with controlled user access and authorization.

Dell Desktop Virtualization Solutions (DVS) enable the secure push of virtual desktops and applications to personal PCs or Macs, seamlessly, providing a productive end-user experience and anytime access to work applications. Dell can also help create an app store on your employees' devices that is separated from their personal apps and data.

Optimizing infrastructure to meet the challenges of mobility

Dell Networking can provide increased bandwidth and capacity across the enterprise for traditional Ethernet as well as wireless devices. Dell Networking solutions are based on industry-standard protocols and can be flexibly added to any network. Dell Networking is simple to install, easy to configure and straightforward to manage. Dell provides validated reference guides and starter kits for enterprise wired and wireless connectivity.

With the ClearPass GuestConnect appliance, IT now has the ability to identify each user, device and application accessing the network. You can offer fine-grained access control to ensure that employees have the right level of access and bandwidth without sacrificing control or security.

Endpoint devices with consumer appeal

Dell's Latitude 10 tablet provides sleek, attractive devices with enterprise-class features that can be marketed to end users as the right device for work and play. Dell tablets are built for business. Windows 8 provides the touch interface end users crave with the applications they need for work. In addition, Dell's XPS notebooks and Ultrabooks merge the consumer desire for notebook devices with enterprise-class features such as encryption with embedded TPM chips that IT approves of and can control.

Dell Services provide a clear differentiator with offers such as Dell ProSupport with 24x7 direct access to Dell Expert Centers for true business support, and Accidental Damage and Theft Recovery services, which provide peace of mind for employees on the go. And, Backup/Restore services provide online backup and restore to give IT additional peace of mind.

Transforming your university

Embrace BYOD proactively; don't just let it happen to you. This trend is an opportunity for you to rethink and modernize your IT strategy and improve the working/learning environment you provide to your students, faculty and staff. ■