Issue Brief

Simplifying Bring Your Own Device (BYOD) in Education

New solutions ease management and ensure security

The Rise of BYOD

Education's digital revolution continues to progress, with increasing numbers of schools, districts and higher education institutions undertaking mobile device initiatives. However, many education leaders struggle with tight budgets and resource shortfalls in the aftermath of the economic downturn, leaving them unable to afford school-owned devices for students and staff at a time when demand for them is increasing rapidly.

BYOD programs, in which students and educators bring personal electronic devices to school for use in academic and administrative work, provide a solution by jointly addressing budget constraints and the consumerization of technology.

The definition of BYOD can vary greatly from campus to campus, but most often includes:

- Students or staff using their personal devices at school
- Allowing students and staff to bring any personally owned device(s) into the classroom to support school procured or dictated standardized devices

Education institutions across the country are turning to BYOD solutions to better enable and provide the benefits of technology — such as digital education resources to enhance learning and improve student and staff productivity — while avoiding the cost of owning the devices themselves. The downside, however, is that users are not under the direct control and scrutiny of the IT department, opening the door to concerns around privacy, data sharing, device management, network security and more.

This Center for Digital Education issue brief helps K-12 and higher education institutions assess the issues and challenges around BYOD so they can better bring BYOD benefits to students and staff, while simultaneously ensuring effective management and security.

The Issue with BYOD

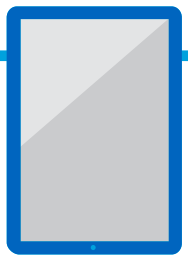
Education institutions implementing BYOD must take steps to alleviate privacy, security and regulatory concerns, of particular importance to K-12 institutions responsible for student users who are underage.

Allowing personally owned devices to access the network can open the door to breaches of privacy and data security, as student- and staff-owned devices may lack the necessary protections and features to keep information safe.

Additionally, while BYOD has the potential to significantly reduce capital expenditures, it can dramatically increase operating expenditures if not properly deployed and managed. IT departments must confront these issues, as well as deal with a potentially unlimited number of different operating systems and applications on devices with either unique security features or none at all.

Big Numbers on BYOD

81% of Gen Y prefers to connect wirelessly, according to the Pew Research Center, which recommends merging this preference with education strategies.[1]



Most college and university students (**86%**) **own laptops as their primary computer device** for academic purposes, but more students in 2012 than in previous years owned tablets (**15%**), **smartphones** (**62%**) **and/or e-readers** (**12%**).[3]

According to a Project Tomorrow Speak Up Survey released in October 2012, **nearly 50 percent of high school students and 40 percent of middle school students own or have access to a smartphone or tablet** — a *400 percent* increase since 2007.[2]

A Center for Digital Education (CDE) survey of **nearly 150 IT professionals in K-20 education revealed that 85 percent of faculty and staff bring a personal device** to work (laptop, tablet or smartphone) which they use to access their school or college's network.

There is an encouraging and very worthwhile flipside, however. With a well-defined BYOD solution, IT personnel can ensure security policy conformance for all devices connecting to the network, reduce time needed for general IT infrastructure upkeep, reduce spend, increase student and staff productivity, and satisfy the demand for mobile access and rich media content.

The Solution to Effective Management and Security

While BYOD issues abound, smoothing implementation and ensuring security is relatively simple with new management solutions.

Security

Protecting users' privacy and information, as well as the integrity of the institution's network, is of utmost concern. From the start, flexible network access control must be set up to provide access only to intended users (students, teachers and staff) and to prevent security breaches and hacking/theft of sensitive data.

BYOD security tips:

- ✓ Focus on data, apps, users and devices.
- ✓ Consolidate user rights monitoring into a single engine to provide a comprehensive picture of a user's activities from the time the user enters the campus (virtually or physically), as well as when and how the user accesses each system, application and piece of data.
- ✓ Monitor proactively. Put controls in place to prevent access to anyone whose behavior triggers an alert.
- ✓ Know the environment. When suspicious activity is detected, analyze all the digital fingerprints to identify the cause of the problem. Utilize reporting tools on all registered device activity.
- ✓ Leverage application monitoring and scanning tools, including manual processes, to help identify security defects in code written by third parties. Use a full-scope SDLC (software development lifecycle)-based review process where needed, as well as governance and auditing, to ensure apps meet compliance requirements.
- ✓ Ensure all users are trained in proper use of network and applications.
- ✓ Draft and communicate easily understood policies around permitted use to counter risks to regulatory compliance, and maintain adherence with Family Educational Rights and Privacy Act (FERPA), Children's Internet Protection Act (CIPA) and Health Insurance Portability and Accountability Act (HIPAA) regulations.

Management

Enforcing consistent network access without triggering a rise in operating expenditures is the balancing act of BYOD management. It is the IT department's job to keep things running smoothly once a BYOD solution has been implemented.

Network access control does more than protect privacy/security — it also guards against network slowdowns and makes sure all devices in use are in compliance with organizational policy and federal and state regulations.

Unified BYOD with HP IMC

The industry's only complete unified BYOD solution delivers the features education providers need most. Unique for its Intelligent Management Center (IMC), HP's BYOD solution offers a single-pane-of-glass network management solution, delivering complete visibility across your entire enterprise network, from the data center to the network edge. Additionally, IMC goes beyond "mere" BYOD by delivering converged management across various networks — physical and virtual, wired and wireless — and applies the appropriate security policies to the users and devices accessing your network. Learn more at hp.com/networking/BYOD.

Additionally, endpoint integrity checks and continuous monitoring of the Wireless Local Area Network (WLAN) — to quickly identify problems/inefficiencies and help ensure optimal network performance at all times — are integral to a well-managed BYOD solution.

BYOD management best practices should include:

- ✓ Management of the infrastructure to support personal devices
- ✓ Identification of personal devices to develop and apply the best policies
- ✓ Policies defined per device and user
- ✓ A self-registration portal for student- and staff-owned devices
- ✓ Simplified deployment
- ✓ Core-to-edge network control
- ✓ Resources management and capacity planning
- ✓ Real-time visibility of bandwidth consumption
- ✓ Auditing of online behavior
- ✓ The ability to capture traffic trends, application and session performance
- ✓ Security policy provisioning and enforcement
- ✓ Network traffic monitoring

With proper management and security, K-20 educational institutions can maximize the benefits BYOD offers.

Endnotes

1. www.pewresearch.org/millennials/
2. www.tomorrow.org/speakup/pr/PR_102212_MobileLearningreport.html
3. www.educause.edu/library/resources/ecar-study-undergraduate-students-and-information-technology-2012