The Policy of BYOD: Considerations for Higher Education

In December 2012, *eWeek* quoted Gartner Vice President Ken Dulaney: “IT has been saying this is the way, but in today’s world the dictator is being overthrown. I’ve been told by organizations that they’re Blackberry only, but then I walk down the hall and see iPads. IT is coming to grips with the fact that they’ve lost control.”

Is the answer to regaining control to establish policy? Retake the dictator’s throne? Impose restrictions? Lock down access? Appoint the IT organization as the self-anointed sheriff in the wild, wild west of BYOD (Bring Your Own Device)? If this is indeed the answer, many are already armed with policy, procedure, and prescription to ensure the sanctity of the “IT homeland.”

However, before drafting more policy, we might be wise to explore the concept of policy and what purpose policy serves in the context of BYOD.

What Is BYOD?
BYOD is one component of the consumerization of technology in the workplace. By its very term, BYOD refers only to the device. Consumerization refers to a broader range of concepts including such topics as services (e.g., Dropbox, Google Drive, Evernote), end-user access to personal cloud services, consumer devices and services provisioned by the institution, and the rapid deployment of “the Internet of Things.”

BYOD is not new. Clearly, the term BYOD has become the latest buzzword of consultants and bloggers, among others. But I am referring to the notion of individuals bringing their own personally purchased devices to campus. Students have been bringing laptops to campus for decades. In many cases, doing so was required by the institution. And who knows how many USB memory devices are plugged in to campus networks right now? All the while, faculty are likely establishing their own networks in their classrooms. Aside from the popularity of the term BYOD, what makes the influx of personal-use devices so novel to the campus that the practice warrants policy? Is it the sudden proliferation of smartphones stuffed in pockets and purses and of tablets carried in messenger bags and backpacks? Or is the overwhelming demand for access truly necessitating some response from the IT organization?

If policy is needed, to what extent does existing policy cover the use of personal devices? Is the institutional Technology Acceptable Use Policy sufficient? Are there other policies that could address concerns related to BYOD, such as a data-standards policy referencing data security? An audit of existing policy may be the place to start.

Why Develop Policy?
Why should a higher education institution go through the typically rigorous and lengthy process that results in policy? What purpose does policy serve?

The answer is that higher education faces a unique set of challenges when addressing the consumerization of technology. Those challenges are differentiated as students, faculty, and staff. Each user group brings with it unique demands. A survey of these user groups would be ideal to determine the services, systems, and data requirements on a day-to-day basis.

Students are becoming increasingly asset-light. What systems, services, or data do they need as a result? To what extent are they being required to access or are they demanding to access mission-critical systems or sensitive data? The *ECAR Study of Undergraduate Students and Information Technology, 2012,* hints at their requirements, with “accessing course websites or syllabi” (66%) and “using course or learning management systems” (64%) heading the list. Does the institution’s existing information and network architecture mitigate a need for new policy?
Faculty are requesting to use their personal iPads and smartphones in the classroom. As the Internet of Things proliferates, other technologies will require Wi-Fi connectivity. Faculty want to leverage the portability, ease of use, and access to device-specific apps that enhance the learning experience and certainly make their lives a bit easier. These are all legitimate reasons for providing faculty with access to Wi-Fi. Similar to students' use of consumer devices, what policy is required to support faculty?

Staff pose a more significant challenge. The question that is most relevant in this case is what systems, services, and sensitive data do staff need to access using their personal mobile devices? A quick survey will most likely reveal that their preference for using their mobile devices is not to access sensitive data, the ERP, or other mission-critical systems/services. Industry surveys indicate how employees currently use their personal mobile devices in the workplace: the top three activities are accessing the employee intranet/portal, accessing e-mail and/or calendars, and reading or viewing documents, spreadsheets or presentations. Similar patterns of use should be considered on college and university campuses.

If policy is determined to be necessary, does each user group require unique policy? How will policy or policies accommodate the ambiguity of emerging technologies that will invariably end up on campuses—in learning spaces, staff offices, and residences? How should the institution draft policy that is sufficiently broad to allow for future technologies yet sufficiently detailed to be enforceable?

Certainly, there is a case to be made for policy that will secure networks, systems, and sensitive data. Policy can also address support for personally owned devices, subsidies for required business use of personal devices, and provisions for institutional liability—among other administrative concerns unique to BYOD.

At What Cost Policy?

Policy brings with it significant costs beyond the human capital invested in the drafting, reviewing, editing, and approval of the documents. Communicating policies to all concerned, monitoring activity and behavior(s), and enforcing prescribed corrective actions all add to the complexity and cost of policy management.

Recently Werner Boeing, CIO of Roche Diagnostics, stated: “People believe that IT is about technology, but it’s really a behavioral science—understanding the behaviors of your company’s staff, leaders, and customers—and facilitating the adoption of a new vision.” Understanding the behaviors of your institution’s staff, faculty, and students may be the best first step to establishing policy. Understanding the culture of the institution is imperative. To what extent does institutional culture influence the desire to establish policy? Is the institutional leadership risk-averse? To what extent do workplace policies influence the development of policy? Understanding the dynamics of trust, mutual respect, and professional confidence will help determine the nature of policy, if required.

If an institution’s culture is driven by policy, there is no shortage of articles, white papers, case studies, and policy templates that can provide a path to BYOD.

If progress and action are the norm on campus, a quick assessment of the infrastructure can establish a next-generation enterprise, always-on middle platform (e.g., Wi-Fi, 4G/LTE, browser, apps, virtualization), ensuring a frictionless experience for the end-user. Returning to Gartner VP Dulaney, the eWeek article noted: “To hear Dulaney speak of BYOD in broad terms, his advice could be mistaken for toddler parenting advice: Give warnings. Set boundaries. Be clear about consequences.”

The takeaway? To each his (her) own. The decisions to develop BYOD policy will vary campus by campus, college by college, department by department, and individual by individual.

Notes
2. All mention of mobile devices is intended to reference personally owned devices, not organization- or institution-provided devices.

Stephen DiFilipo (sdifilipo@gmail.com) is Vice President and CIO at Cecil College.

© 2013 Stephen DiFilipo. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License (http://creativecommons.org/licenses/by-nc-nd/3.0/).