What is BYOD?

BYOD stands for Bring Your Own Device. It is when employees are allowed or encouraged to use their personal mobile devices, including notebooks, phones, and tablets, for work (either on site or off). The term first appeared in 2009 via Intel, but only gained widespread use in later years as other companies began discussing their employees using personal devices at work. In 2012, the EEOC adopted a BYOD policy, ushering the era of this practice in government organizations. Even the White House has a BYOD policy at this point.

According to Tech Pro Research, 74% of organizations either already using or planning to allow employees to bring their own device to work.

Why Should You Care?

Research has shown that even if you are not participating formally in BYOD, it is likely that your employees are already using these devices to do work. Think about your own device usage—do you use your phone to make business calls, send e-mails, or post to social media for your job? When you are at the NJLA conference or an event like today's TechFest, are you taking notes, posting, answering e-mail? If you said yes, you BYOD.

In NJ, BYOD has serious implication for both employers and employees because of the Open Public Records Act. The recent ‘Bridgegate’ scandal involving Governor Christie’s aids sending e-mails about closing of the bridge entrance has highlighted this concern of BYOD. Forbes recently reported:

---

“One thing Gartner emphasizes is the importance of realistic public-sector BYOD policies. The report states, “Government IT organizations may have an illusion of control by either providing and managing those devices or issuing well-articulated policies to allow and manage employee-owned devices. However, the reality is that employees...can decide how much they want to use corporate information and applications versus personal information and applications.” Gryth adds that BYOD can be even more contentious in government offices because employees’ work devices are subject to public records requests.”

What about Privacy? Employee? Patron?

As we move to a mobile world, we are outsourcing more and more library functions to third party vendors—think Overdrive or Zinio. When an employee, or patron, is using their own device are you making it known that they are being tracked by a third party? Does that party sell the information? Are you using “free tools” such as Google products? Have you made the privacy issues clear to your employees?

Resources for Further Research:

NJ State OPRA Information:  http://nj.gov/opra/
exemptions to OPRA:  http://www.nj.gov/grc/public/eoexempt/

IBM: IBM has a nice summary of what BYOD is, what the risks are, and some considerations when creating a policy. Full disclosure, they do sell an Enterprise Product for helping employers to manage BYOD. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html


California Case Law: This case may (or may not) completely change the BYOD landscape. http://www.computerworld.com/article/2599121/byod/california-cell-phone-ruling-poses-big-byod-challenge.html


ACLU Position on Privacy & Technology: https://www.aclu.org/issues/privacy-technology This is a terrific general overview of privacy issues facing humans today, what our rights are in the US, and how to manage these issues. https://www.aclu.org/blog/librarians-privacy this is specifically for librarians!

Public Libraries Online: http://publiclibrariesonline.org/2013/06/is-your-library-ready-for-byod/

Disruptive Library Technology Jester: http://dljt.org/article/advancing-patron-privacy-with-shared-understanding/ This is a fantastic blog post on how to protect patron privacy while using third-party vendors.