Checklist: Create a BYOD policy for your team
Create a BYOD policy for your team

Letting employees use their personal smartphones at work can be convenient for everyone, but it can also put your company data and assets at risk. Protect yourself by drafting a bring-your-own-device (BYOD) policy.

Use this checklist to craft a policy that supports your security needs and addresses typical employee privacy concerns.

- **Define acceptable use on the clock.** Who should be permitted to use a mobile device at work? A helpful tool for some may be dangerous or distracting for those operating machinery that requires their full attention. List examples of the work-related activities where smartphones can boost efficiency. Also decide which personal activities are acceptable on company time—
perhaps brief phone calls and emailing, but not playing games. You may want to explicitly prohibit any device use while driving.

- **Set boundaries on phone features and data transfers.** One of the most important functions of a BYOD policy is to plug potential leaks of business data. Some businesses restrict use of smartphone cameras on-site to protect intellectual property or others’ privacy. If your business handles sensitive data, consider rules that limit employees from transferring data to personal devices unless it’s encrypted. Check that the policy you establish in this area is specific and dovetails with any regulations your business must follow when handling client, customer, or patient data.

- **Cover cybersecurity rules.** Mobile devices can provide an entry point for malware, or if lost or stolen, literally put access to your data into the wrong hands. Your policy should require employees to use the strongest access controls available on their device, and you may ask them to set up a location-based tracking app such as “find my iPhone.” Consider banning “jailbroken” devices that have been tinkered with to bypass the manufacturers’ controls and limiting app downloads to official app stores. List procedures you want employees to follow if they lose their device, starting with reporting the loss to you promptly.
○ **Detail employees’ privacy expectations.** Make sure your policy discloses how using their devices for work may impact staffers’ privacy. Will you potentially monitor their activity on your company network, for example? If you expect staffers to provide access to their device, describe the circumstances when you would ask this, and what will and won’t be accessed.

○ **Keep your policy on the right side of the labor laws.** Any time that employees spend using their personal devices for work purposes, outside of their regular hours, could potentially count as overtime. If you have hourly-paid workers who are eligible for overtime, you might decide to exclude them from your BYOD program altogether. Or, you might include in your policy the requirement that they use a time-tracking system to properly log all hours. Consult your legal counsel to determine the right steps for your business.

○ **Spell out what you’ll pay for.** Are you willing to cover some, all, or none of an employee’s voice or data plan? Some courts have ruled that employers who require employees to use their personal devices for work have to pay a reasonable portion of the costs. Your policy should be clear on whether BYOD is mandatory or an employee convenience that’s allowed if staffers follow your rules. Some employers pay for roaming or additional data
charges if use is mandated, such as when an employee is traveling for work. Be clear and consistent on reimbursements.

- **Address departing employees.** Employees who leave the company will be taking along a personal device that may have had access to your proprietary data, so your policy should include a plan for cleanly terminating that access. Describe how you’ll disable connections to business data and resources, as well as your procedure for remotely wiping any company data from devices when staffers leave.

- **Explore mobile device management.** MDM technology can help reduce some of the risk associated with BYOD: It separates work data from personal data and helps protect critical business data. There are numerous MDM options, as well as mobile application management products, that are tailored for small businesses. Most let you remotely lock down and wipe data on lost or stolen employee devices—critical for businesses that handle sensitive data. If you decide to require installation of this software, your policy should specify what information may be deleted and define employees’ responsibilities for keeping their personal data backed up.

- **Review your draft policy with an expert.** Once you’ve considered the points above and decided how you’re going to handle each one, write out your
BYOD policy—the Society for Human Resource Management is a useful source for sample policies. Ask your lawyer or HR consultant to read it over to be sure that it satisfies legal and labor concerns before you implement it. Once it’s done, print out copies for all staff to sign and keep it available as a reference tool for when questions arise.