

BYOD Policy Template

Have the final text reviewed for your state before anyone signs; it is a starting point, not legal advice.

Part 1: Scope, Eligible Devices and Security Minimums

[Company Name] Personal Device Policy, effective [Date]. In this policy, "the Company" means [Company Name] and "you" means the employee.

1.1 Purpose and scope. This policy covers personal phones and tablets you use to reach [Company Name] email, chat, files, or accounts. It does not cover anything else on your device.

1.2 Participation. Using a personal device for work is voluntary. The Company offers [a company phone / desktop-only access] to anyone who prefers not to.

1.3 Eligible devices. Your device must still receive security updates from its maker. Jailbroken or rooted devices are not allowed.

1.4 Security minimums. Keep a screen lock with a passcode or biometrics, keep automatic updates on, and use multi-factor authentication on work accounts. Install apps only from the official app stores.

1.5 Lost or stolen device. Report a lost or stolen device to [Policy Owner] within [24] hours.

1.6 Who to ask. Questions about this policy go to [Policy Owner] at [contact].

Part 2: What the Company Can Access, and What It Won't

2.1 What the Company can access. The Company can access only your work accounts and work data, plus the device details its tools show by default (such as model, operating system version and whether a passcode is set, and, with some tools, the serial number or part of the phone number). Under full device management, it can also see the items listed in 2.6.

2.2 What the Company will not access. The Company will not look at your personal email, messages, photos, contacts, browsing history or the content of your personal apps.

2.3 No monitoring or location software. The Company does not install monitoring or location-tracking software on personal devices enrolled under this policy, and it does not use location data from your device.

2.4 No personal passwords. The Company will never ask for the passcode to your personal device or the passwords to your personal accounts.

2.5 If tools change. The Company will tell you in writing before any change in what it can access on your device.

2.6 What the tools manage [If you use app-level controls:] The Company manages only the work apps.

2.6 [If you use full device management:] The Company can see the device details listed in 2.1 and [the list of installed apps, if its tool collects it], with location reporting switched off in its settings. It can erase the whole device only under clause 3.3.

Part 3: Lost Phones, Remote Wipe and Leaving the Company

3.1 Lost or stolen device [If you use app-level controls or full device management:] After the report of 1.5, the Company removes its work data and access from the device.

3.1 [If you use written rules only:] After the report of 1.5, the Company cuts access to your work accounts; you must remove the work accounts, you may erase the device if you choose, and you confirm the removal in writing.

3.2 Selective removal first. Wherever its tools allow it, the Company removes only work accounts and work data, not your personal data.

3.3 Full wipe only with separate consent. The Company will erase your whole device only if you have signed the separate wipe consent in the agreement. It will tell you before it does, unless the device is lost or stolen.

3.4 Back up your own data. You are responsible for backing up your personal data; the Company is not liable for personal data lost in a wipe you agreed to.

3.5 Leaving the Company. On your last day, you remove work accounts and apps from your device, with [Policy Owner] present if you agree. Your confidentiality duties continue after you leave.

3.5 [If you use app-level controls or full device management:] The Company also removes its access and work data remotely.

3.5 [If you use written rules only:] The Company cuts access to your work accounts, and you confirm the removal in writing.

Part 4: Costs and Work Outside Working Hours

4.1 Who pays. The Company pays [a monthly stipend of [Amount] / a share of your phone bill on request] to employees who use a personal phone for work.

4.2 State rules (a note for you; delete it from the copy). Some states, California among them, require employers to reimburse work expenses; in California that includes a reasonable share of a personal phone bill used for work. Under federal law, work costs the employer requires an employee to bear may not push pay below the minimum wage.

4.3 Damage and repair. Your device remains your property, and repairs are your cost unless [Company Name] agrees otherwise in writing [or your state requires the Company to pay].

4.4 Work outside working hours. You are not expected to read or answer work messages outside your working hours unless you are on call. If you are paid hourly, time you spend on work messages is work time and is paid.

For salaried exempt staff, the pay rules differ, so ask whoever reviews the policy how 4.4 applies to them.

BYOD Agreement: The Signature and Wipe-Consent Form

Acknowledgment. I have read the [Company Name] personal device policy dated [Date] and agree to follow it[, including the enrollment of my device under clause 2.6].

Employee name: [Name]; Device (make and model): [Device]; Date: [Date]; Signature: [Signature]

Separate wipe consent (optional; it may be left unsigned). I agree that [Company Name] may erase my whole device under clause 3.3. I understand this removes my personal data too.

Wipe consent signature: [Signature]; Date: [Date]

Company representative: [Name]; Signature: [Signature]; Date: [Date]

Source: <https://www.hoverwatch.com/blog/for-business/byod-security-policy/>, version 2026-10-22