BYOD policy

☝ This is a sample Bring Your Own Device (BYOD) policy for employers that allow or require employees to use their own electronic devices, such as smartphones and tablets, for work. This policy can be incorporated into an employee handbook or a comprehensive information security policy, or also used as a stand-alone document. This template applies only to private workplaces and is jurisdiction neutral. Please note that state or local laws may impose additional or different requirements, but this BYOD policy template can serve as a useful and relevant starting point for your team. Be sure to consult with a lawyer before rolling out any BYOD policy.

To save a copy of this template in Google Docs, click “File” → “Make a copy”.

[Company XYZ] grants its employees the privilege of using their own personal electronic devices, including but not limited to smartphones, tablets, and computers of their choice (“devices”) at work for their convenience. [Company XYZ] retains the right to revoke this privilege if users do not adhere to the policies and procedures outlined below.

This policy is intended to protect the security and integrity of [Company XYZ] data and technology infrastructure.

[Company XYZ] employees need to agree to the terms and conditions outlined in this policy to be able to access company resources. This policy applies to work performed on a device on [Company XYZ]’s behalf during working and non-working hours, on and off of [Company XYZ]’s premises.

No expectation of privacy

All material, data, communications, and information, including but not limited to email (both outgoing and incoming), telephone conversations and voicemail, instant messages, and internet and social media postings and activities created on, received, or transmitted by, printed from, or stored or recorded on the device for [Company XYZ]’s business or on behalf of [Company XYZ] (“[Company XYZ] content”) is the property of [Company XYZ], regardless of who owns the device(s) used.

You are expressly advised that in order to prevent misuse, [Company XYZ] reserves the right to monitor, intercept, review, and remotely wipe, without further notice, all [Company XYZ] content, in [Company XYZ]’s sole discretion. Therefore, you should have no expectation of privacy whatsoever in any [Company XYZ] content.

By signing this policy, you understand and consent to [Company XYZ]'s monitoring, intercepting, reviewing, copying, disclosing, and remotely wiping all [Company XYZ] content, in [Company XYZ]'s sole discretion. You also agree that the use of any device for [Company XYZ]'s business or on behalf of [Company XYZ] is at your own risk and [Company XYZ] will not be responsible for any losses, damages, or liability arising out of the use of any device for [Company XYZ]'s business or on behalf of [Company XYZ] under this policy, including any loss, corruption, or use of any content or loss of access to or use of any device, its software, or its functionality.

Acceptable use

[Company XYZ] defines acceptable business use of devices as activities that directly or indirectly support the business of [Company XYZ].

The company defines acceptable personal use of devices on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others

Employees may use their mobile devices to access the following company-owned resources: email, calendars, contacts, documents, etc.

The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)

Do not use social media while on your work time unless it is work related as authorized by your manager.

New employees and/or contractors won't be granted access to any [Company XYZ] systems until after they have completed all HR onboarding tasks, which may include but are not limited to the signed employment agreement, intellectual property agreement, and information security policy.

[Company XYZ]'s policies prohibiting harassment, discrimination, and retaliation apply to the use of all devices under this policy. You may not use any device in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religion, or any other characteristic protected by federal, state, or local law.

Non-exempt employees using their own devices under this policy are not permitted to use their devices for work purposes during non-working hours without prior written authorization from [Company XYZ].

Any employee who discontinues use of their device under this policy or leaves [Company XYZ]'s employ must allow [Company XYZ] to remove any [Company XYZ] content, work product, or sensitive business information from their device and disable any software or services provided by [Company XYZ] on their device.

[Company XYZ] prohibits employees from talking, texting, emailing, or otherwise using a mobile or other electronic device, regardless of who owns the device, while operating vehicles, machinery, or equipment of any kind.

Acceptable use for in-office teams

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to (include examples such as not secure websites)

Devices and support

Smartphones, including iPhone, Android, and Windows phones, are allowed (be as detailed as necessary with models, operating systems, versions, etc.). Tablets including iPad and Android are allowed (including models, operating systems, versions, etc.).

Rooted (Android) or jailbroken (iOS) devices are strictly not allowed to access the network or any company resources.

Connectivity issues with company resources are supported by IT; employees need to contact the device manufacturer or their carrier for any operating system or hardware-related issues.

Devices and support terms for in-office teams

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software, and security tools before they can access the network.

Smartphones and tablets belonging to employees that are for personal use only aren't allowed to connect to the network.

Reimbursement

[Company XYZ] will do one of the following (include any bullet points you decide to incorporate in your policy):

- reimburse an employee for X% of the cost of the device (include the total amount of the company's contribution)
- contribute X amount of money toward the cost of the device

- cover the cost of an entire data plan and/or provide a virtual business number an employee can use for all work-related communication on their existing devices
- pay half of the phone/data plan

The company will (or will not) reimburse the employee for the following charges: roaming, plan overages, etc.

To be eligible for reimbursement, employees may be required to submit a copy of their monthly statement or bill, as applicable, substantiating the costs incurred on the employee's device. For more information on device reimbursement procedures, please contact [person/position].

Security

Control and management of individual user passwords is the responsibility of all [Company XYZ] personnel and third-party users. To prevent unauthorized access, devices must be password protected using the features of the device, and a strong password is required to access the company network/or any company resources.

Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers, and symbols. Passwords must change every 180 days and the new password can't be one of 15 previous passwords.

The device must lock itself with a password or PIN if it's idle for five minutes.

Employees' access to [Company XYZ] data is limited based on user profiles defined by IT and automatically enforced.

The employee's device should be remotely wiped if any of the following occurs:

- the device is lost
- the employee terminates their employment IT detects a data or policy breach
- a virus or similar threat to the security of the company's data and technology infrastructure

Software programs purchased and provided by [Company XYZ] are to be used only for creating, researching, and processing materials for [Company XYZ]'s use. By using [Company XYZ] software (and networking systems if applicable), you assume personal responsibility for their use and agree to comply with this policy and other applicable [Company XYZ] policies, as well as city, state, and federal laws and regulations.

All software acquired for or on behalf of [Company XYZ], or developed by [Company XYZ] employees or contract personnel on behalf of [Company XYZ], is and will be deemed [Company XYZ] property. It is the policy of [Company XYZ] to respect all computer software rights and to adhere to the terms of all software licenses to which [Company XYZ] is a party.

You may not illegally duplicate any licensed software or related documentation. Unauthorized duplication of software may subject you and/or [Company XYZ] to both civil and criminal penalties and liability. To purchase software, obtain your manager's approval. All software acquired by [Company XYZ] must be purchased through X department.

Risks/Liabilities/Disclaimers

If a remote wipe of a device needs to be done, it's the employee's responsibility to take additional precautions, such as backing up anything saved to the hard drive to avoid losing personal data.

Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use their devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.

The employee is personally liable for all costs associated in the event they need to replace their device. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Confidentiality and proprietary rights

[Company XYZ]'s confidential information and intellectual property, including trade secrets, are extremely valuable. Employees must treat them accordingly and not jeopardize them through their use of their devices. Disclosure of [Company XYZ]'s confidential information to anyone outside of the company and use of [Company XYZ]'s intellectual property is subject to the company's [insert name of confidentiality/proprietary rights agreement or policy].

Further, any work product created, stored, or maintained by you on your device is subject to [Company XYZ]'s [insert name of confidentiality/proprietary rights agreement or policy].

Violations of policy

If you violate this policy, you will be subject to corrective action, up to and including termination of employment. If necessary, [Company XYZ] will also advise law enforcement officials of any illegal conduct.

Termination of employment

Upon termination of employment, you must log out of all company resources including any software used during your employment.

Work-life balance

Team members are not expected or encouraged to reply to emails, calls, or any other form of communication outside business hours unless it’s an emergency.

For Slack (or internal communication tool used), team members are encouraged to mute their notifications outside of business hours. For team members that utilize a business number to communicate with others, they must have an away voicemail greeting set up that clearly states when a caller can expect to hear back from them.