Bring Your Own Device (BYOD) Policy

Objective

This policy establishes [Company Name] guidelines for employee use of personally owned electronic devices for work-related purposes.

Scope

Employees of [Company Name] may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops and computers.

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the human resource (HR) department for more details.

Procedure

Device protocols

To ensure the security of [Company Name] information, authorized employees are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. [Company Name]'s IT department must install this software prior to using the personal device for work purposes.

Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites.

All employees must use a preset ringtone and alert for company-related messages and calls. Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.

Restrictions on authorized use

Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. [Company Name] policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on nonwork time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Managers reserve the right to request employees' cellphone bills and use reports for calls and messaging made during working hours to determine if use is excessive.

Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. [Company Name] reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.

An employee may not store information from or related to former employment on the company's application.

Family and friends should not use personal devices that are used for company purposes.

Privacy/company access

No employee using his or her personal device should expect any privacy except that which is governed by law. [Company Name] has the right, at any time, to monitor and preserve any communications that use the [Company Name]'s networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that [Company Name]'s resources in these areas are being use according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

Company stipend

Employees authorized to use personal devices under this policy will receive an agreed-on monthly stipend based on the position and estimated use of the device. If an employee obtains or currently has a plan that exceeds the monthly stipend, [Company Name] will not be liable for the cost difference.

Safety

Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked or damaged equipment

Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.

In an effort to secure sensitive company data, employees are required to have “remote-wipe” software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.

[Company Name] will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. If IT is unable to repair the device, the employee will be responsible for the cost of replacement.

Employees may receive disciplinary action up to and including termination of employment for damage to personal devices caused willfully by the employee.

Termination of employment

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

Violations of policy

Employees who have not received authorization in writing from [Company Name] management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow [Company Name] policies and procedures may result in disciplinary action, up to and including termination of employment.