Sample Mobile Device Policy

Published by:

AGJ Systems & Networks Inc.
14257 Dedeaux Rd.
Gulfport, MS 39503
228-392-7133
www.agjsystems.com

Disclaimer and Legal Notices:

While all attempts have been made to verify the information provided in this policy and accompanying materials, neither the Author nor the Publisher assumes any responsibility for errors, inaccuracies, or omissions. Before implementing these strategies, you must be aware of the various laws governing business transactions, marketing, or other business practices in your particular geographic location as some of the suggestions made in this document may have inadvertently introduced practices deemed unlawful in certain states, municipalities, and countries. This policy is not intended for use as a source of legal, human resources or accounting advice. In all cases, you should consult the services of a professional, licensed

attorney in all matters pertaining to the operation, delivery, and protection of your business and services.

SAMPLE MOBILE DEVICE POLICY

Purpose

This policy outlines the use of mobile devices by employees of [Company Name]. This policy should be read and understood by all employees who:

- Want to use, or are using, a personal mobile device for work purposes
- Use a company owned mobile device
- Bring a personal mobile device onto company property

Policy

Use of personal mobile devices: Employees may have the opportunity to use their personal devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include, but are not limited to, personally owned cell phones, tablets, laptops and computers.

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

Employees will receive an agreed-upon monthly stipend to use personal devices 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. The device remains the property of the employee who is responsible for all repairs or replacement of the device.

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

Use of company owned mobile devices: Certain employees may be issued a company owned mobile device. Use of these devices is contingent upon continued employment with [Company Name] and the device remains the sole property of [Company Name]. Company provided mobile devices are part of a 'family plan' with shared minutes and include data usage. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a Payroll deduction for personal usage.

Security: Employees must put a PIN, password or other security measures in place on every device that is used to access company information. Further, employees are required to have mobile device management (MDM) software installed on their personal mobile devices as recommended by [Company Name]. This software will [list what the software does here, e.g., monitor all emails, text messages and photos, along with the physical location of the device]. This software must be installed by the IT department prior to using the device for work purposes.

When possible, employees should use two-factor or two-step verification for added application/device security.

Employees may not use any cloud-based apps or backup that allows company-related data to be transferred to unsecure parties (see "approved app list" at the end of this document). Due to security issues, mobile devices may not be synchronized to other devices in the employee's home. Making any modifications to the device hardware or software, or installing additional hardware or software, beyond authorized and routine installation updates is prohibited unless approved by the IT department. Employees may not use unsecure Internet sites.

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

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.

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

Behavior: 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 policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to the use of personal devices for work-related activities.

Excessive personal calls, e-mails, or text messaging during the work day, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on non-work 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.

Mobile devices shall be turned off or set to silent or vibrate mode during meetings, conferences, and in other locations where incoming calls may disrupt normal workflow.

Work Hours: Nonexempt employees may not use their mobile devices for work purposes outside of their normal work schedule without authorization in advance from management.

This includes but is not limited to reviewing, sending, and responding to e-mails or text messages, responding to calls or making 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.

Privacy: No employee 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 utilize [Company Name]'s networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to determine proper utilization, regardless of the ownership status of the device used to access the company's networks. Management reserves the right to review, retain, or release personal and company-related data on mobile devices to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze usage patterns and may choose to publicize this data to assure that [Company Name]'s resources in these areas are being utilized according to this policy. Furthermore, no employee shall knowingly disable any network software or system identified as a monitoring tool.

Inspection: *At any time, the employee may be asked to produce the mobile device for inspection. The purpose of these inspections is to insure that the employee is following company policy.*

Safety: Employees are expected to follow applicable state or federal laws or 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 mobile 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. The only exception to this stipulation is if the call can be placed or accepted entirely hands-free. Special care should be taken in situations where there is traffic, inclement weather, or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of mobile 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 mobile devices as doing so can potentially be a major safety hazard.

Lost, Stolen, Hacked, or Damaged Equipment: Employees are expected to protect mobile 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 (MDM) installed on their mobile devices by the IT department prior to using the devices for work

purposes. This software allows all data to be erased remotely in the event the device is lost or stolen. The remote wipe process will remove all programs and data from the phone and reset it to factory defaults. [Company Name] will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or remote wiping. Employees must notify management immediately in the event their mobile device is lost or stolen.

If the mobile device is damaged, the employee must notify management immediately. The employee will be responsible for the cost of repair or replacement.

Employees may receive disciplinary action up to and including termination for damage to company owned mobile devices caused willfully by the employee.

Termination of Employment: Upon resignation or termination of employment, the mobile device will be reset to factory defaults using the remote wipe software. [Company Name] will not be responsible for loss or damage of personal applications or data resulting from the remote wipe.

Approved App List

App Name	Function/Purpose

Signed by: _____ Date: _____

REMEMBER TO HAVE YOUR ATTORNEY REVIEW THIS DOCUMENT.