THE STRATEGIC SOLUTION
A Grace Hill Company

+ SightPlan®

Bring Your Own Device

Sample Policy & Agreement

Statement

To enjoy the benefit of technological advances in the industry and to promote convenience and efficiency for our associates, the company has established a Bring-Your-Own-Device (BYOD) Program. This program allows eligible and approved associates to use their own mobile devices for business tasks, including the use of work-related tools, such as email and work-related apps.

As with any use of technology, the company must protect the security and integrity of its data and technology infrastructure, while also balancing associate privacy concerns, wage and hour laws, safety, and other legal concerns.

Policy

General

- The company will determine eligibility criteria for associates who wish to participate in the BYOD Program. Eligible and approved associates may use their personal electronic devices ("devices") for work-related tasks and may use work-related apps as approved by management.
    - These devices may include smartphones, tablets, and computers (including laptops).
    - Eligible associates approved for the BYOD program must comply with all terms and conditions of the BYOD User Agreement and any related policies prior to connecting a device to the company network, downloading any work-related apps onto a device, and using a device for work-related purposes.
    - Associates are expected to use their device(s) in an ethical manner and adhere to applicable policies as outlined in the Employee Handbook and other company manuals, including but not limited to:
        - Nondiscrimination and anti-harassment Confidentiality
        - Employment – Overtime
        - Employment – Meal Breaks, Travel, and Training Time Conduct – Behavior
        - Conduct – Computers and Other Resources Conduct – Company Property

Sample Policy

- Conduct – Personal Calls and Visits Safety – Operating Vehicles
- Social Media

- The company uses [Enter here the type of security software being used.] technology as part of its technology security protocol.
- All business data on the device is the property of the company, and associates must agree to access it through company email or approved applications only.
- The company reserves the right to inspect the devices belonging to associates participating in the BYOD Program at any time. Only authorized members of management, HR, or IT may inspect an associate's device. The company may disconnect devices from the company network and/or disable work-related services if a device is lost, stolen, or missing. When possible, IT will notify the associate in advance. Associates are responsible for backing up their personal information in case of inadvertent wiping.
- Nothing in the BYOD program is intended to prohibit an associate's rights under the National Labor Relations Act, as outlined in Employment at Will.
- This policy supersedes all previous versions or agreements regarding the BYOD policies.
- Failure to comply with the various terms and conditions may result in no longer being able to use a device for work, as well as disciplinary action up to and including termination.

Approval and Access

- Management and IT must review and approve all user requests for use of the company's security technology.
- Approved associates must have [Insert name of security software here.] and anti-virus software installed on their devices by IT prior to using the company network and accessing company data from their personal devices.
- Access to company data is based on user profiles as defined by management and IT.

IT Department Responsibilities

- The IT department will:
  - Keep a record of all approved user access.

- Provide associates support for security and connectivity issues.
- Implement proper corporate data security measures when there are software or hardware modifications to a device.
- Remove any company data from personal devices when employment ends.
- Make reasonable attempts to respect the privacy of the associate when inspecting the device for business data.
- Refrain from examining the elements of the device that are not essential for work-related activities.
- Remotely wipe a device if it is lost, the associate terminates employment without first permitting IT to inspect the device, or IT detects a data or policy breach, a virus, or threat to company data. In doing so, the IT department will implement reasonable provisions to protect the loss of personal data.

Reimbursement

- Qualified associates may be eligible for reimbursement of the cost for the device, accessories, and monthly phone/data plan as outlined in the BYOD User Agreement.
- An associate participating in the BYOD program must repay [Company Name] in full and within 30 days of employment termination, if the employee:
- Is terminated or resigns, and within the last 12 months, [Company Name] reimbursed the associate for the full cost of a device (and/or accessories) or made up-front device plan payments.

Procedure

- Obtain permission from your supervisor and the IT department to access the company network.
- Review and execute the BYOD User Agreement with your supervisor.
- Work with the IT department to ensure that all applicable security software is installed on your device.
- Complete all required expense reports (if applicable) to ensure reimbursement for your device, accessories, data, or any other applicable costs.

Resources

- BYOD User Agreement

Bring Your Own Device Employee User Agreement

[Company Name] allows eligible associates to use their personal electronic devices for business. Associates who choose to participate in the BYOD Program must understand the company will take measures to protect the security and integrity of its data and technology infrastructure, while also balancing associate privacy concerns, wage and hour laws, safety, and other legal concerns.

Your failure to comply with the various terms and conditions of the [Company Name] BYOD Program, as described below, may result in no longer being able to use a device for work, as well as disciplinary action up to and including termination.

Sample Agreement

As a participant in the BYOD Program, you must:

- Obtain written approval (through the execution of this user agreement) from your manager and the IT Department to participate in the BYOD Program. Only the following approved devices will be allowed to access the network.
- [Insert list of supported devices here.]
- Use your device(s) in an ethical manner and adhere to applicable policies as outlined in the Employee Handbook and other company manuals, including but not limited to:
  - Non – Discrimination and Anti-Harassment
  - Confidentiality
  - Conduct – Computers and Other Resources
  - Conduct – Behavior
  - Conduct – Personal Calls and Visits
  - Conduct – Company Property
  - Social Media
  - Employment – Meal Breaks, Travel, and Training Time
  - Employment – Overtime

- Safety – Operating Vehicles

- Understand that:
  - [Company Name] reserves the right to inspect your device at any time. Only the Regional Manager, Vice President, HR Department, or IT Department may inspect an associate's device.
  - All business data on the device is the property of [Company Name] and must be accessed through approved software only.
  - The IT Department may remotely wipe your device if it is lost; you terminate employment; or IT detects a data or policy breach, a virus, or threat to company data.
  - In the event the device needs to be wiped, the IT Department can generally accomplish this while leaving your personal data intact. However, this cannot be guaranteed; therefore, take appropriate steps to back up personal emails, photos, contacts, videos, etc.
  - You may be blocked from accessing certain website or apps during work hours or while connected to the company network.
  - Nothing in the BYOD program is intended to prohibit an associate's rights under the National Labor Relations Act, as outlined in the [Company Name] Employment at Will policy.

Preparing Your Device

Ensure you have security and anti-virus software installed on your device by the IT Department prior to accessing the company network and data from your personal device(s).

- Provide the IT Department with your mobile number in the event of an emergency.
- Maintain your device's original operating system, and keep all updates current.
- Ensure your device is password protected, and/or use the biometric fingerprint authentication (“touch ID”).
  - Passwords should be difficult to guess; do not use personal information patterns that a person could reasonably determine.
  - Based on the device, passwords, if possible, should be at least eight

characters long and a combination of upper and lowercase letters, numbers, and symbols.

  - Passwords should be changed every 90 days. New passwords should not be the one of the previous 10 passwords.

- Ensure your device self-locks if idle for longer than two minutes.
- Install a non-offensive screensaver on the device, lock screen, and background. For questions, contact HR.

Securing Corporate Data

- When communicating with other associates, customers or vendors from a personal device, use business software (the corporate email account, instant messaging, etc.) or approved applications only. Personal email and text should not be used for business communications at any time.
- Do not store business data on your device, including property photos and community information. If data is unintentionally downloaded on your device (by viewing email attachments or by other means), you must delete the files.
- Be mindful that your personal device that you use for company purposes contains proprietary company information. As such, the device should remain in your sole possession, be solely for your use, and you should take all possible measures to protect company information on the device. If you feel that you must share your device with others, contact your supervisor who will determine, along with the IT Department, whether a company-issued device may be provided to you.
- Rooted (android) or jailbroken (IOS) devices are not allowed to connect to the company network due to security and bandwidth issues.
- Notify the IT Department:
  - Before downloading any business software to your personal device; ensure that there are no copyright violations, or other licensing requirements.
  - Prior to any hardware or software modification outside of regular system updates.
  - Immediately following a suspected data breach or unauthorized access of the device.

Employee Privacy

- [Company Name] will make reasonable attempt to respect your privacy by accessing the device only for justifiable business purposes. These include, but are not limited to, installing security software, complying with court-ordered requests for information, safeguarding company intellectual property, and executing company business.
- [Company Name] will not monitor areas of your personal device that are not necessary for work, such as personal email, photos, and personal applications.

Acceptable Use

- Follow all applicable laws and regulations regarding the use of your device.
- Work Use
    - During paid work time, use the device only for work-related purposes. All time spent using the device for [Company Name] business purposes is considered work time and must be paid.
    - Non-exempt associates should not use their device to conduct [Company Name] work after work hours or during unpaid breaks unless the associates are on call or have received approval for overtime from their manager. This includes reviewing, sending and responding to emails or text messages, responding to phone calls, making phone calls, or utilizing other installed business applications.
    - Refer to the [Company Name] Employment – Overtime and Employment – Meal Breaks, Travel, and Training Time policies.
    - During approved leaves of absence, associates may not use their devices for [Company Name] work matters without prior management approval. [Company Name] may suspend the associate's access to corporate data, as well as reimbursement for the device, while the associate is on leave.
- Personal Use
    - Do not use your device for personal matters during paid work time (such as emails, Facebook, shopping, internet surfing, etc. or items unrelated to work). Follow the company's Conduct – Personal Calls and Visits policy.
    - Do not use the device for other outside business activities during company work hours, or to store/transmit proprietary data belonging to

another company or a former employer.

Employee Reimbursement

You agree to the following reimbursement amounts:

- Cost of Device (client will select appropriate statement)
    - [CompanyName] will not purchase or reimburse you for the cost of the device or any related accessories.
    - [Company Name] will reimburse you for $_____ amount towards the cost of the device, as well as limited accessories including phone charger, protective case and earbuds. If you resign or are terminated from [Company Name] within 12 months of such reimbursement, you must repay $Name within 30 days of employment termination.
- Cost of Monthly Plan (client will select appropriate statement)
    - [Company Name] will not reimburse you for the monthly phone/data plan.
    - [Company Name] will reimburse you for a portion of your monthly phone/data plan. Reimbursement is based on your position and estimated use of the device.
    - $CompanyName will reimburse you up to $_____ of the monthly phone/data plan.
- Other Device Costs (client will select appropriate statement)
    - [Company Name] will not reimburse you for the following charges: roaming, plan overages, etc.
        - Exceptions include roaming charges or other fees incurred for business such as international travel.
- [Company Name] will reimburse you for the following charges: roaming, plan overages, etc.
- [Company Name] will/will not reimburse the cost of a privacy screen.

Safety

- Do not use the device while walking, driving, conducting potentially dangerous or hazardous work, or any work that might be adversely affected by use of the device.

- Follow the company's Safety – Operating Vehicles policy.
- Associates charged with traffic violations due to device use while driving are responsible for all liabilities related to such actions.

BYOD Issues or Problems

- Contact IT for security and connectivity issues. If you accidentally download prohibited files, contact the IT Department for instructions on removing the information.
- If you need access to company data outside the scope of your user profile, discuss the issue with your manager.
- For repairs or problems with hardware or software, contact the device manufacturer or carrier.
- If your device is lost, stolen, or damaged:
    - Report the issue to [Company Name] immediately and no later than 24 hours after the event.
    - Notify your mobile carrier immediately upon the loss/theft of your device.

Upon Exit from [Company Name]

- You will cease accessing company data stored on your device. If the company requests, you agree to delete all company data from your device.
- You may be asked to produce the personal device for inspection, retrieval of company data, and removal of third-party software by [Company Name] at the time of your exit.
- You will maintain your mobile number.

If you resign or are terminated from [Company Name] within 12 months of being reimbursed for the total cost of your device by [Company Name], you are required to repay [Company Name] 100% of the cost within 30 days of employment termination.

By signing below, you are entering into the BYOD Agreement with the company. You must ensure that you read, understand, and fully comply with the Agreement and all company BYOD requirements, as set forth above. If you fail to abide by the requirements or breach any part of the Agreement, you will no longer be entitled to participate in the BYOD program and may be subject to additional discipline.

Sample Agreement

Employee Name

Supervisor Name and Title

Supervisor Name and Title

Employee Signature

Supervisor Signature

Date