
# Personal Mobile Device Acceptable Use Policy

## Training Slideshow

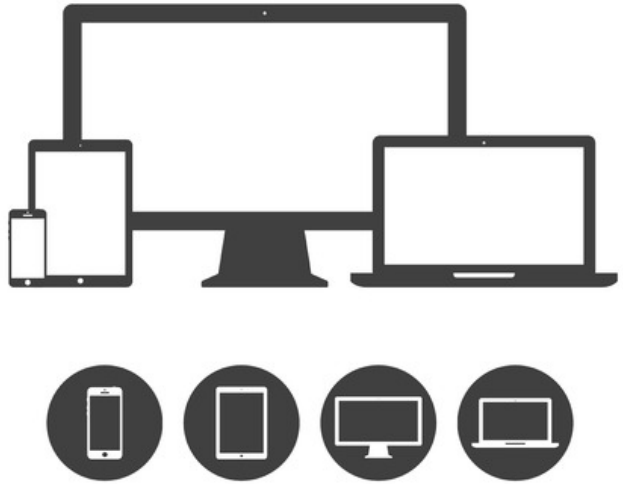
# Instructions for Using This Template

- Replace [company] with your company's name, and other company-specific information in [square brackets].
- Ensure that all policies are applicable to your company's goals.
- Review [optional] items and delete if they do not apply.
- Replace the footer with your own.
- Delete this slide.

# What are Personal Mobile Devices?

Primarily smart phones, but also includ

- Ultra-mobile/netbook computers.
- Personal laptop computers.
- Portable gaming devices.
- Portable media devices.
- Tablet computers.
- e-Readers.



Any personally-owned device storing corporate data and/or connecting to [company]'s network is bound by the acceptable use policy.

# Purpose

- Permitting you to use your own devices to work is mutually beneficial, allowing you to be accessible and productive on a device you are already familiar with.

- However, personal devices introduce potential risks to the integrity of private information and business data that is made available when connected with [company]'s data and technology.

- The acceptable use policy is necessary to mitigate the risk.

- By connecting a personal device to [company]'s network, you agree to comply with the policy explained here, and grant [company] permission to erase the information on your device when necessary. This may include erasing personal data in some cases.

# Case Study: John at the Beach


- John is at the beach with his family when he receives a sensitive e-mail from a coworker on his personal iPhone.
- John quickly responds to the email and continues with his day at the beach.
- Later that day, John realizes he forgot his iPhone on the counter at a food stand at the beach.

- Realizing he has lost his phone, John immediately calls his manager and the IT contact responsible for managing mobile devices.
- IT is able to remote wipe the iPhone immediately, mitigating data leakage risk and the effect it may have on the company.

- John's quick action ensured sensitive data was protected from access by an unintended party.
- The net effect in real dollar terms to the company is $0 outside of the cost to set up the initial infrastructure.
- John buys a new iPhone and loads a backup image of his previous device onto it, minimizing the time required to return to productivity.

Quick action by employees that have lost devices is the most effective way to mitigate security threats from personal mobile devices. The faster [company] can remote wipe the device, the better.

# Responsibilities

- You, as an employee of [company], are responsible for acting in accordance with company policies and procedures.

- Connections between mobile devices and the corporate network *will* be managed by [company]'s IT department.

- [Company]'s IT department will *not* directly manage the functionality or performance of devices except in their capacity to connect to the corporate network.

- Users are expected to adhere to the same security standards no matter where the device is used.

# Policies: Access

Mobile devices must be used appropriately, responsibly, and ethically. In most circumstances, these goals can be reached by following the policies laid out here.

Mobile devices must be approved by IT before being connected to the corporate network.

If necessary, devices must be modified or set up to meet [company]'s security standards.

Virtual Private Network (VPN) software must be used when accessing the corporate network from outside the workplace.

# Policies: Security
## *Do*

**Devices must be encrypted with a strong password.**
A PIN code is not sufficient.

**Use reasonable physical security measures.**
Do not leave your device unattended.

**Use anti-virus / anti-malware software.**
If a mobile device connects to a computer, have anti-virus on the computer.

**Store Crypto Keys In Separate Location**
Never store USB crypto keys with the device it unlocks.

# Policies: Security
## *Do Not*

**Do not store unencrypted passwords.**
For example, by e-mailing a password or storing it in a text file.

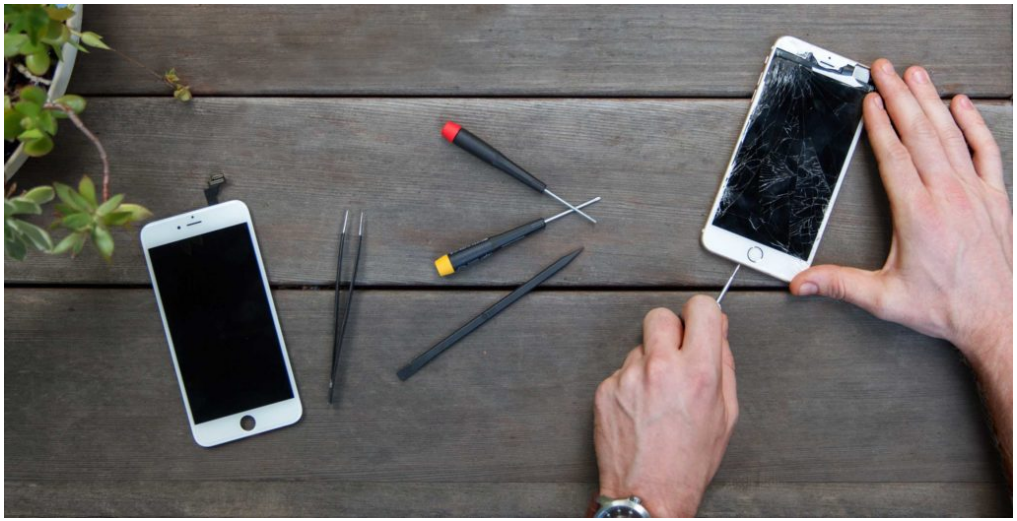
**Do not try to bypass security measures from IT.**
Leave additional software in place.

**Do not leave company data on your device indefinitely.**
If you stop using the device or end your employment, erase company data.

**Do not use location-based services.**
Sharing your location with third-parties is not allowed.

**Do not use your device to capture media.**
Avoid pictures, video, or audio on company property.

# Policies: Support



[Company] will provide limited support for sanctioned devices

**Supported:** can't access corporate e-mail, calendar, collaboration.

**Not supported:** phone won't turn on, screen is cracked, no service.

IT may limit access.

Your ability to transfer data to and from specific resources on the corporate network may be reduced at any time.

# Policies: Organizational Protocol

Your activity will be monitored while on the company network.
For example, dates, times, and duration of access.

[Company] [will / will not] reimburse the cost of devices.
[Policy and maximum amount of hardware reimbursement].

[Company] [will / will not] reimburse the cost of services.
[Policy and maximum monthly amount of data and voice usage reimbursement].

# Incidents

Incidents involving devices that contain corporate data – such as a lost or stolen device, or suspicion of unauthorized access – must be ***immediately*** reported to your manager and the IT department.

# Policy Enforcement Technology

## Remote Wipe

By connecting to [company]'s network and taking the necessary security measure, you agree to grant IT the ability to erase all data on the device, if it is necessary to do so to preserve [company]'s security and integrity.

## Encryption

Data on the device and data transferred to and from [company]'s network must be encrypted. Contact the IT department to ensure that the required level of data encryption is present.

## Third Party Software

[Insert details if 3rd party software is used for mobile device management and enforcement.]

# Consequences of Non-Compliance

- The [Responsible Title] will be advised of breaches in the policy and is responsible for remediation.

- Failing to comply with these policies and procedures may result in one or more of the following:

| | | | |
|---|---|---|---|
| Suspension of technology use at the company. | Loss of connection privileges. | Disciplinary action. | Termination of employment. |

# Questions?

- A copy of the *Personal Mobile Device Acceptable Use Policy,* reviewed here, must be signed before connecting any personal devices to the corporate network.

- The *Remote Wipe Waiver* must also be signed before connecting personal devices.

- This policy is available for future reference at [location].

- Questions or comments about the policy should be directed to [name, phone number, e-mail].