



Acceptable Use

**How to Write a Mobile Policy Document
Employees will Actually Follow**

Build a Strong Usage and Security Policy for Mobility

A mobile computing policy document (sometimes called an Acceptable Use Policy) tells employees what's expected of them when it comes to using smartphones, tablets and other mobile endpoints for work. It marks out the responsibilities of the company as well.

These policies serve multiple purposes – but the most important are:

- Protecting corporate data and assets.
- Allowing productivity, accessibility and collaboration to happen safely, whenever and wherever it benefits the company.

Mobile device users need rules and guidelines to understand what safe mobile computing means – generally, but in the context of your organization specifically. A good policy not only provides employees with the information they need to safely access your networks and systems, but also tells them how to manage, resolve or redirect any issues that do come up. A well thought-out policy document gives you a solid framework for any device ownership model. Forming your policies also forces you to think through the various aspects (including business and legal issues) before you get too far down the path.

The level of detail in these policies can range from broad statements on appropriate access to more specific aspects like reimbursement for cellular network charges, which devices are acceptable, secure use best-practices and a walk-through of risks, liabilities, and disclaimers.

An important note:

It's worth the effort it takes to create a mobile policy document that your employees can actually understand. Most of the examples you'll find in enterprises today are written in legalese. The document should certainly be reviewed and approved by your legal team, but that doesn't mean it should be impenetrable to the people who need to use it.

If your users are put off by your policy document and fail to understand it, they'll be reluctant to use their devices to their full potential. That means you're leaving opportunities on the table. And if they don't understand their responsibilities on the security side, you open your organization up to unnecessary risks. A clear, plain-language guide is the best way to ensure you safely get the most out of your investment in mobility.

How to Use This Document

Use this document as a template to build your policy document. Walk through each section, consider the options you have and the stance you want to take. Talk through the implications with all the relevant players (including Legal). This list of topics is not exhaustive but provides a solid start – just copy and paste the sections that make sense for your business, then add to it and tailor it as you see fit.

Content that's in callout boxes or [square brackets] is for your guidance – remove in the final document.

Mobile Policy Document Template

Here, provide a general statement explaining why you've created this policy document.

What this document is about

For example:

Mobility is an increasingly important part of this company's strategy to boost productivity, collaboration and access to critical information. But all this has to be accomplished safely. This document explains what's expected of you when it comes to the way you use mobile devices for work. It also explains what you can expect from the company, and from IT. And it outlines what to do if things go wrong – when a device goes missing, for example.

We've made it as concise as possible. Since you're asked to sign it to acknowledge you understand it and agree to it, please do take the few minutes you'll need to read through. As you might expect, employees who don't abide by these policies face reprimands and penalties of various kinds, all the way up to termination. If you have questions, contact mobilepolicy@brand.com to get answers.

Lay out the basic guidelines that apply to all mobile device users, regardless of who owns the device.

Using mobile devices:

Your responsibilities for all devices

For example:

You agree to do your part to protect the company network and the confidential data that's stored on, or accessed using, a mobile device. How? By taking steps like these:

- Doing your best to protect the device from going missing (by loss or theft).
- Reporting a lost or stolen device right away.
- Keeping the operating system and apps up to date. Checking with IT if you're not sure how.
- Using only approved apps and tools to access company data. [\[Link to a list\]](#)
- Using the security programs and practices IT provides to prevent hacking and/or changes to security software/settings.

Provide high-level direction to users who carry out work using their own mobile devices.

For devices you own (also called BYOD — Bring Your Own Device)

For example:

We invite you to use your own smartphone and/or tablet for work. But because our IT department doesn't manage or maintain these devices, it's critical that you follow the guidelines in this document. As the device owner, it's your job to:

- Register the device with IT before you start using it for work.
- Settle any service or billing problems with the carrier (the network).
- Keep the device current by installing software updates/patches when they become available.
- Install any software that your manager agrees is required for business use (but only from the approved software list provided by IT).
- Keep any relevant warranty information.
- Replace the battery if and when that's required.
- Perform all data, settings, media and application backups.

Provide guidance for users who do their work with a company-owned device, but also use that device in their personal lives. In COPE scenarios, IT commonly has the same controls it does over corporate-only devices. Generally, IT and the company agree to leave users' personal content alone unless they have specific cause to interfere. When advanced containerization capabilities are in place, IT can often stay completely out of users' personal content.

For devices the company owns, that contain your personal data too (also called COPE, for Corporate Owned, Personally Enabled)

For example:

COPE smartphones and tablets are managed by IT.

You're responsible for:

- Installing/agreeing to software updates that are made available by IT.
- Reporting a lost or stolen device immediately.

You can download apps from popular app stores, install software you want or need, and store photos, videos and music etc. The company will make every attempt to respect COPE user privacy. But remember, this is a company-owned device. You must be aware that the device may be wiped remotely or reset if it's thought to be compromised in any way. See the section "Monitoring and protecting" for more detail.

This section sets out IT's areas of responsibility. It also sets expectations for users as to what IT can do depending on the ownership model, so BYOD users aren't surprised when IT directs them back to their carrier for certain support issues.

What you can expect from IT Support Services

For example:

For devices you own (BYOD), IT will:

- Make sure your device is compliant with our security standards. If it is, they'll register it under your name and then set it up to access approved company applications and networks.
- Configure your email, calendar and contact syncing service.
- Configure your Wi-Fi® access.
- [Etc.]

This section outlines who can access corporate networks and data via mobile devices – including partners, suppliers and other guests. It should tell employees how to go about requesting access on behalf of these third parties. Note that you'll want to develop an acceptable-use document for these individuals too.

Who's eligible for mobile access?

For example:

- Anyone who wants mobile access to our network or data via mobile device must request approval from a senior manager.
- Not every user will have the same permissions or access levels. You might encounter restrictions based on your role or department.
- When suppliers, contractors and guests are given access, their privileges will be limited. To request access for an outside partner, please contact IT and submit the Guest Network Access Request form. [\[Link to the form\]](#)

Even when there's a clear separation between work and personal data on a mobile device, (containerization or sandboxing), provide clear direction on what's okay and what isn't.

What you can and can't do on the corporate network

For example:

- We've restricted access to certain websites and applications. This list changes all the time, but you can ask IT for the latest version if it's available.
- While you're connected to the corporate network, remember:
 - You must not use a device(s) to store or transmit illicit material or proprietary information belonging to another company.
 - Do not text or email while driving. It's prohibited by the company, independent of any local laws. Only talk on a mobile device while driving if you're using a hands-free set.
 - On devices where there is a clear and secure container (or 'sandbox') for business data and/or applications, company policies will apply only to the work-related data and applications, and any corporate network access.

List out the devices that are currently acceptable, including software versions, models, and any specific instructions based on the type of device. Mark out any distinctions in ownership model – for example, you may not supply corporate-owned Android devices but may allow BYOD Android use.

Devices we currently support

For example:

For BYOD devices (where you own the device):

- BlackBerry® 10; iOS 10 and 9; Android™ 7 and 6 devices are currently permitted.
- Once you've submitted your request for network access and it's been approved by your manager, contact IT. They'll configure the device for use with our standard work applications (like email, office productivity software and security tools) and any special approved apps or software your role requires.
- IT will be able to provide support for any issues you may have with work tools or with getting connected to the corporate network. For any issues that relate to the device itself, handle those as you would any personal mobile device you own (for example, call your service provider or network carrier). If you're not sure what the problem is, start with your provider – they'll be able to tell you if it's something they can fix or not.

Explain that only approved devices are allowed access, no matter what the ownership model. You may also want to talk about how users can request that IT add a certain device to the list.

Devices we don't currently support?

For example:

The following device platforms are not supported at this time:

- iOS 7, 8 or earlier; Android™ 4, 5 or earlier
- If you're not sure whether your personal device is supported for use at work, check the full list of supported devices [\[Link to it\]](#). If it's not named there, it's not supported. You can raise the issue with IT to find out whether your device may be supported soon – the list is updated regularly as new devices become available and older ones become obsolete.

Included here are the specific actions and precautions users must take to ensure secure device network access and data protection. This material will also describe how your mobile device management system works, in terms of what it may require of users, and how it may affect the user experience.

How to do your part for mobile security

For example:

As we've indicated in this document, mobile access to work networks and data comes with responsibilities, whether you own the device or the company does. What must we all do as mobile workers?

- Make reasonable attempts to avoid malware and viruses by only installing trusted apps and software, to keep devices from being lost or stolen, and to ensure sensitive data isn't lost or compromised.
 - Leave the security controls that IT implements alone.
 - Ensure the device is password-protected. A strong password is also required to access the company network. What makes a strong password? It must have at least six characters and a combination of upper- and lower-case letters, numbers and symbols, with a minimum of one capital letter and one symbol. You'll be required to change your password every 60 days and the new password can't be one you've used in the last 12 months.
 - Make sure the device is programmed to lock itself with a password or PIN if it's idle for five minutes.
 - After ten failed login attempts, the device must lock. You'll need to contact IT to regain access.
 - Don't use rooted or jailbroken devices to access the network. These are devices that have had limitations and protections removed so that users can add things like unauthorized software.
 - Ensure, where possible, that the device is configured to securely separate corporate data from personal data.
 - Don't try to connect with smartphones and tablets that aren't on the company's list of supported devices.
 - Don't connect smartphones and tablets you own for personal use that aren't registered with IT.
- Make sure your device is configured to encrypt content. Only devices that have this capability are on the approved list.
 - Be sure you have the right approvals. Your mobile access to company data depends on the approvals you have from management – often it's a function of your job role or department.
 - Report a lost or stolen device right away by contacting IT and your manager. Although we take all the best security precautions, the more time that elapses between the loss of the device and IT finding out about it, the greater the risk that company data could fall into the wrong hands.
 - Know that your device may be remotely wiped if 1) the device is lost, 2) you leave the company, or 3) IT detects a data or policy breach or other threat to the security of the company's data or technology. When possible, only the corporate data will be wiped, unless you give IT written approval to wipe your personal content too. [Link to the written approval form]
 - Keep the device operating system and corporate applications software current.

Consult with Legal here especially, for intent and wording.

Monitoring and protecting

For example:

The company has the right to:

- Monitor the applications and content in the corporate (containerized) area of your mobile device.
- Remotely wipe or reset the device to factory default. Where personal and corporate data and applications are kept separate, every attempt will be made to wipe only the corporate data and applications (unless you ask us to wipe your personal content as well).
- Remote wipe may be required if the device is lost, stolen or believed to be compromised. The device can also be wiped if it's found to be non-compliant with company policies, or you're no longer affiliated with the company.

Provide details on who will pay for the device, the data plan, overages, roaming charges etc.

Reimbursement

For example:

The company will reimburse you for the initial cost of two mobile devices, up to \$200.00 each. You can buy a device that's more expensive, as long as it's on the list of acceptable devices, but you'll need to pay the difference. As you probably know, you can drive down the cost of the device by signing on to a longer voice and data plan (2 years, for example).

You'll need to buy the device first, then submit the enrollment form [Link to it]. Your reimbursement check will be issued within 10 business days once it's been approved by your manager.

You can upgrade devices every 18 months, and claim the same amount (\$200.00) with each upgrade.

If available, describe what users can and should do through self-service capabilities prior to seeking any IT Help Desk involvement. Describe users' responsibilities for backing up data, and how to engage IT or your MDM/EMM solution in backup and restore scenarios.

Self-service device management

For example:

The company provides a tool you can use to handle certain admin tasks for your devices. For example, if your device is lost or stolen, you can use this web-based app to remotely change the password or delete data from your device. You don't need to install any software on your computer to use the tool. IT will provide you with the web address and login information.

Provide guidance on acceptable mobile device use while travelling. Address any responsibilities, highlight high-risk countries and detail any required post-trip practices.

International travel rules

For example:

The company will cover long distance or travel expenses you incur as you work. These may include:

- Long distance calls you need to make for business.
- Roaming or long distance charges you incur while you're travelling on business. We ask you to do your best to minimize these costs – using Wi-Fi, for example, instead of cellular data while you're travelling. In some cases, in agreement with your manager, IT may disable international roaming to keep costs down.

You'll want to engage the legal department to help fill in this section as serious privacy and liability issues are involved.

Risks/liabilities/disclaimers

For example:

- We reserve the right to disconnect devices or disable services without notification.
- If your device is lost, stolen or compromised, report it immediately, but certainly within 24 hours. If you own the device but use it for work (BYOD), it's your responsibility to notify your mobile carrier (the service provider) if your device goes missing, and to wipe the device of any and all work-related content if you have the capability.
- You're expected to use your device in an ethical and legal manner always, and to follow the company's acceptable use policy (outlined above).
- If you're found to be non-compliant with any of the policies in this document, know that the company reserves the right to take appropriate disciplinary action, up to and including termination.

Enforcement

For example:

Any user found to have violated the policies in this document may be subject to disciplinary action.

They may:

- Be denied access to the corporate networks, applications and data.
- Have data removed from the device.
- Lose their job.

Remember to add a signature area so you have a record of each employee's agreement to the policy.

_____ Employee	_____ Date
_____ Manager	_____ Date

Mobilize Your Business Simply and Securely

With the BlackBerry Enterprise Mobility Suite, enterprises can say “yes” to their users’ and business leaders’ demands for anytime, anywhere productivity through secure mobile apps.

The BlackBerry Enterprise Mobility Suite provides consistent multi-platform endpoint and app management policies and controls across iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry® platforms, no matter the device ownership model or the user groups being mobilized.

The BlackBerry Enterprise Mobility Suite provides a turnkey solution for rolling out collaboration apps, line of business apps, custom apps and/or leveraging your existing Microsoft® apps, all while protecting your business and your employees’ privacy. BlackBerry-secured apps have consistent containerization and security policies across operating systems and devices to keep work and personal content separate. When an employee leaves the organization, only the BlackBerry-secured apps and business data are wiped from the device. All personal data remains personal and the rest of the device is left intact.

Learn more at www.blackberry.com/suite

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world’s most sensitive data across all end points — from cars to smartphones — making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo,

Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols “BB” on the Toronto Stock Exchange and “BBRY” on the NASDAQ. For more information, visit us.blackberry.com.