Guidelines for Creating Your Company's Mobile Use Policy

Table of Contents

PART 1:

What Is A Mobile Use Policy?

Photo Source: http://jquerybyexample.blogspot.com/2011/08/mostly-asked-jquery-interview-questions.html

A mobile use policy is a policy within your company that serves as a guideline for employers and employees alike, detailing out how mobile devices (including laptops, smartphones, tablets, etc.) are allowed to be used with regard to company materials and data. It also discloses the penalties involved should any of these policies be violated.

PART 2:

What Needs To Be Included In A Mobile Use Policy?

Photo Source: http://www.page1solutions.com/page-1-blog/are-you-using-website-checklist.html

There are a few sections that need to be included in your mobile use policy. The first one is BYOD.

BYOD stands for Bring Your Own Device. The basic idea is that employers have the choice between two scenarios.

One, they allow employees to use their personal devices (laptops, smartphones, tablets) for work purposes, both in and out of the office. This is the scenario of a BYOD environment.

Two, the company provides employees with devices that are strictly to be used for work. Employees are not allowed to use the company devices for personal matters, and they are not allowed to use their personal devices for company matters. This scenario is not a BYOD environment, since the company supplies the devices.

To learn more about BYOD, you can read this blog post: *Pros and Cons of BYOD.*

These days, given how many devices people have, and how many different types of devices are out there (not to mention the expense), more companies are allowing employees to work from their own devices.

The next section needs to cover what type of data is allowed to be present on people's personal devices.

If you are providing employees with devices, this section doesn't matter too much, since your company actually owns the devices.

However, if you have a BYOD environment, this section is very important, and the policies are going to depend a great deal on the type of data your company deals with.

The most basic type of data is email. It is the main way we communicate with each other, and most people are not able to do their jobs without access to email. So, if you are not even comfortable allowing your employees to have their work email account on their personal devices, a BYOD environment is really not for you.

Next is other types of data– mainly the shared drives. If you are using a cloud-based program to handle your shared files, it becomes very easy to access those files from anywhere. Many cloud programs even have apps so that people can access their files from a smartphone or tablet– like Egnyte, Google Drive, and Dropbox.

The last section needs to be about data on a laptop. There are a few different ways employees can work out of the office– Remoting in to their work computer, a VPN connection, or a cloud-based program.

This blog post will give you more insight into how each of these scenarios works:

How To Work From Home

Regardless of how employees are working from home, one thing needs to be clearly spelled out in your mobile use policy– who owns the data.

Ideally, if an employee is working from a personal device they are only going to store company data on company shared drives, not to their personal machine. However, that is not realistic, and there is no way to enforce that.

Instead, it needs to be understood and agreed upon by both parties that regardless of where the data is stored, if it is company data it belongs to the company– not the individual.

Another section that should be included here is what an employee is allowed to do with their personal device, if they are using it for work purposes as well.

While you technically don't have a right to tell someone what to do with their personal property, you also want to be sure that your company data is not associated with a device that takes part in any illegal activities.

PART 3:

What Happens When the Employee Moves On?

Photo Source: http://www.123rf.com/photo_17905049_3d-people--man-person-hold-a-black-briefcase--businessman.html

It's really rare that an employee will stay with just one company forever. It is natural that after some time an employee will either decide to move on from the company, or will be asked to leave.

Either way, when the employee leaves there is a lot of work to do—and what happens to the data on their devices needs to be a big part of that.

So now we have come to the big questions that all employers are worried about. What happens to the data when they leave? How do I get it back? Mainly– Who owns the data?

This is why your mobile use policy needs to be very clear. Make sure to cover each section thoroughly, so that there are no questions when the time comes.

One note that should be made here is that while it is really important to have a policy that details out what happens when an employee leaves, inspections of mobile devices are usually done when an employee starts working with the company as well.

A section of your policy needs to say that if an employee is going to be using their personal devices for work purposes, the company has the right to inspect those devices before the employee starts using them for work purposes, and make sure they approve of them– that there is nothing illegal, and no information from a former job still on them.

Now, let's discuss what to put in the policy for when an employee decides to move on.

First, make sure it is understood that their work email account needs to be removed from their devices. This is very simple to do, and the employee can do it themselves.

There are also things you can do on your end to ensure that no more messages will be sent to that email account, and that the former employee no longer has access, such as immediately forwarding the emails to a new account and/or changing the password to the account.

Next, if the employee had any apps on their devices that were being used for work, such as Dropbox or Egnyte, make sure that those apps are deleted.

If the employee was using these programs for personal use as well (which is less likely with Egnyte than with Dropbox), make sure that all work accounts are deleted.

In fact, when an employee sets up a file-sharing account, make sure it is separate from their personal one. This clear distinction will make it much easier to quickly get all company data off the devices when the time comes.

Now comes a trickier part– laptops.

Although your mobile use policy may have detailed out that an employee was only allowed to save files on company shared drives, regardless of whether or not they were working from home, the big question becomes...how do you know that's what they did? We have already mentioned that this expectation is unrealistic with today's technology, and virtually impossible to enforce.

If they did, removing all work data from their computer becomes very easy– you can simply delete those files from their computer, and/or block their access to those drives.

But what if they didn't? How do you know? And how can you make sure?

This is where your mobile use policy needs to be very careful and clear.

You could include a section that says that if an employee used their personal laptop (or any device) for work purposes, you as the employer are allowed to check through that laptop and make sure that no company information remains.

However, this could present an issue and you might experience push-back from employees who say it is an invasion of their personal property.

Still, you want to have them sign some type of agreement that says you are allowed to make sure no company data remains on personal devices.

One way to do this is to use a feature known as "remote wipe" that exists for mobile devices. Basically, this feature is exactly what it sounds like– it makes it possible to remotely wipe a mobile device of all data.

Certain programs have this feature included, so that when an employee leaves you as the employer can do something- like remotely delete all traces of work email that were on their mobile device.

This leads us to two other things that need to be detailed out in this policy– how long an employee has after they leave the company to remove all work data from personal devices, and what happens if they don't.

Determining how long an employee has to delete company data from a personal device is going to be a decision that will likely be based on the nature of your company's data. You might decide to give them a week, or you might determine that they only get 24 hours to get all company materials off their computers. After that, if the employee can't prove that all work data is off their devices, the company has the right to remotely wipe the machines.

What Happens if They Violate the Policy?

This is a section that defines what will happen if you discover that an employee, or former employee, has violated this mobile use policy. Most likely, it will involve legal action.

It is important that this section of the policy specifies both current and former employees.

While the mobile use policy may seem to concentrate a lot on what to do when an employee is leaving, having guidelines for how to use mobile devices when they are current employees is just as important.

And, especially important is to have agreed upon rules and consequences should this policy be violated. Current employees need to be just as careful, if not more so, than those who don't work at the company any more.

Not to mention that even after an employee has left your company, they still could be carrying around sensitive company information in the one place you can't delete it from– their mind. You have to protect your company from that too.

PART 4:

Where Do I Put A Mobile Use Policy?

Photo Source: http://www.modernmanagers.com/EmployeeHandbook/tabid/1623/Default.aspx

Your mobile use policy needs to be a part of the initial paperwork you give your employees to sign when they are hired.

If you have an employee handbook, make sure there is a section dedicated to the mobile use policy.

And most important, make sure the employee signs the policy, indicating that they read and understood everything.

We recommend having at least a place on the mobile use policy page where they have to put their initials.

These policies are becoming more and more relevant, and you need to make sure your company's data is protected, even from your own employees

PART 5:

Conclusion

Photo Source: http://www.d-trail.co.ke/blog/courier-services/let-your-courier-business-stand-out-from-the-rest/

One final piece of advice in creating your mobile use policy– hire a lawyer to help. You want to check and double-check that everything you put in your mobile use policy is legal by the laws of your state, and that you are not going to leave any loopholes that a disgruntled former employee could possibly take advantage of.

Hiring a lawyer to help is even more important if your company is national or international, because the laws can change from region to region, and you have to make sure you are covering all your bases.

Protecting company data needs to be a big priority for any business. The rise of technology advancements has contributed to a great deal of efficiency and convenience for businesses, but with that rise in convenience comes a decrease in security. To read more about that, check out this blog post:

Why Your Company Needs A Mobile Use Policy

Technology is an integral part of every business these days, and business owners need to make sure that not only are they using technology to help their businesses, but they are taking the necessary steps to protect their business as well.

703.264.7776

www.networkdepot.com