Bring Your Own Device

**Introduction**

Where necessary COMPANY will authorise employees to purchase and use smartphones and tablets of their choosing at work for their convenience. COMPANY reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of COMPANY’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Employees availing of this scheme must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

**Policy Scope:**

The policy applies to all employees of COMPANY.

**Acceptable Use**

Acceptable personal use on company time is defined as reasonable and limited personal communication or recreation.

Employees not authorised from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.

The company has identified the following sites/services/apps as being unauthorised:

* Example 1
* Example 2
* Etcetera…

This list is not exhaustive

The company reserves the right to restrict device camera and/or video capabilities when while on/off-site.

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

**Devices and Support**

Smartphone and tablet devices Operating on the iOs, Windows and Android platforms are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.). Devices that are not on the company’s list of supported devices are/are not allowed to connect to the network.

Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

**Reimbursement**

The company will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the company’s contribution),

or

The company will contribute X amount of money toward the cost of the device.

The company also agrees to pay the following with regards to the service plan…

**Security**

Devices must be password protected using the features of the device and a strong password is required to access the company network.

The company’s strong password policy is:

* Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols.
* Passwords will be rotated every X days and the new password can’t be one of X previous passwords.

**Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network**.

Employees will be prevented from downloading, installing and using any app that does not appear on the company’s list of approved apps.

The employee’s device may be remotely wiped if:

1. the device is lost
2. the employee terminates his or her employment
3. IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

While the company’s IT department will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.

**Liabilities**

Lost or stolen devices must be reported to the company within 24 hours. Employees retain responsibility for notifying their mobile carrier immediately upon loss of a device. The employee is always expected to use his or her devices in an ethical manner and adhere to the company’s acceptable use policy as outlined above. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Failure to comply with the details outlined in this policy may result in disciplinary sanction up to and including dismissal in line with the company Disciplinary policy.