

CoffeeCapulus: BYOT Policy

JOSEPH WILLIAMS

Policy Summary:

This policy is created in order to define acceptable use by staff members using their own devices when accessing and / or modifying company information and data. At CoffeeCapulus, we want staff to be comfortable when working, because of this we are enabling the use of personal devices in order to maximize comfort and efficiency.

All devices that are to be connected to the network will have a company created anti-virus/malware software installed which also includes email protection by default. This software will be administrated by the company IT department and will NOT be able to store any personal information. Privacy is very important to us at CoffeeCapulus, so we take the utmost pride in our methods to protect staff data.

Supported Operating Systems:

Windows 10 or above

MacOS Catalina or above

Android 10.0 or above

Apple IOS version 13 or above

Chrome OS version 80.0.3987.158 or above

Audience intended for the policy:

- All users accessing the business in any way using their own devices.
- Any internal or external auditor that is employed to review the process.

Assumptions:

As all staff have received GDPR training, it is assumed that all staff members have awareness for the GDPR and are fully aware of the consequences of the loss of company personal data.

BYOD / BYOT:

BYOD / BYOT also known as 'Bring Your Own Device / Technology' is staff members bringing devices that they are the owner of in order to access the company's systems whether that is on company property or working remotely.

User:

A user can be anyone who is able to access the company via their devices, this includes but is not limited to:

Staff members, internal reviewers, external reviewers, company executives, or any person who has been authorized to access the company's systems.

Acceptable Use:

- Devices should only be used for business activities that directly or indirectly support CoffeeCapulus.
- Employees are blocked from accessing specific websites while connecting to the company network. Some examples of blocked websites include:
 - <https://twitter.com/>
 - <https://www.youtube.com/>
 - <https://www.twitch.tv/>
 - <https://www.facebook.com/>
 - <https://www.instagram.com/>
 - <https://www.reddit.com/>
 - <https://www.ebay.co.uk/>
 - <https://www.amazon.co.uk/>
 - <https://cardiff.craigslist.org/>
- When on site, all camera and video capabilities are disabled.
- Devices should never be used to do the following:
 - View / download inappropriate content
 - Harass other individuals or groups
 - Engage in activities not related to business e.g. (Selling items online, blogging etc...)
 - Etc.

Allowed apps / software:

- The following software / apps can be installed on devices that are used to access company data:
 - Weather apps
 - Approved productivity apps
 - News apps
 - Mail apps

Banned apps / software:

- The following software / apps should NOT be installed on devices that are used to access company data:
 - Social media apps
 - Movie / TV series apps
 - On-demand video apps e.g. BBC iplayer, My5, etc...
 - Tik Tok / other streaming apps
 - Inappropriate apps e.g. Adult content
- CoffeeCapulus has a zero-tolerance policy when it comes to using devices when driving. Only hands-free should be used when driving in order to avoid accidents.

Device security measures:

In order to ensure that the employees' device has correct protection, the employee must make sure they follow and / or do not ignore the following points.

- All devices connected to the company network are required to have a strong password (combination of special characters, upper case / lower case characters and numbers). The password should be changed every 3 months to a password that has not been used for the past year, this is to ensure security.
- If the employee's device has been idle for more than 3 minutes, it must auto-lock. (This can be done within the mobile devices' system settings).
- Jailbroken / rooted devices are forbidden and should not be used within the network.
- If the incorrect login is used more than 3 times, the device will auto lock and would need IT support to unlock.
- Employees are disallowed permission to download any app that is not on the approved app list stated in the CoffeeCapulus policy.
- Employees personal devices should not be used to connect to the company network.
- Employees access to company data is limited and is dependent on the user profiles that are setup by IT.
- The company will provide staff with a company-certified VPN service for work devices that will allow staff to access data that is tagged as sensitive.
- When a device is connected to the network, all USB ports will be disabled in order to prevent any accidental or malicious data loss / theft.
- At any time, the company can completely wipe a device remotely if the device has been lost / stolen or if the employees contract has expired with the company.
- The employee's device can and will be wiped if the following occur:
 - The device is lost
 - IT detects a data breach
 - IT detects a breach in policy.
 - The employee terminates their employment.
 - IT detects malware / viruses / any potential threat on the device.

Liabilities / Disclaimers:

- The user is responsible for the user to take precautions in order to prevent any loss of personal data from being lost if there are any issues that the IT staff cannot fix / prevent. The employee can do this by ensuring adequate back-ups are set up.
- CoffeeCapulus have the right to disconnect staff devices and / or disable services without prior notification.
- All people connecting their devices to the CoffeeCapulus network are expected to use their devices ethically and in compliance with CoffeeCapulus user policy.
- If an employee's device is lost / stolen, they are required to report the loss within 48 hours. The employees are responsible for contacting their mobile provider immediately when they have lost the mobile device.
- Employees are fully liable for all costs associated with their device and are fully liable for all potential risks including, but not limited to, the loss of data, both company and personal due to any operating system crashes, bugs, viruses, malware and/or any hardware or software problems that would render the device unusable.
- CoffeeCapulus reserves the right to seek disciplinary action if this policy is not adhered to.

By signing this document, I understand and agree with all policies and procedures within CoffeeCapulus' BYOT policy. I also fully understand and accept any consequences that will occur if I break any of these policies.

Signature: