October 2023

**Bring your device to work policy**

# Version history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Name** | **Date Amended** | **Summary of Changes** | **Status** | **Name** |
| **1.0** | 2023-0-06 | Draft version creation | Draft | Ags Angelides |
|  |  |  |  |  |
|  |  |  |  |  |

# Contents

[Version history 2](#_Toc147917235)

[Contents 3](#_Toc147917236)

[1. Purpose 4](#_Toc147917237)

[2. Applicability 4](#_Toc147917238)

[3. Definitions 4](#_Toc147917239)

[4. Expectation of privacy 5](#_Toc147917240)

[5. Acceptable use 5](#_Toc147917241)

[6. Devices and support 6](#_Toc147917242)

[6.1. Provisioning your device for company use 6](#_Toc147917243)

[6.2. When do you not need to provision your device 7](#_Toc147917244)

[6.3. Provision expiry 7](#_Toc147917245)

[6.4. Changing personal devices 7](#_Toc147917246)

[6.5. Currently supported operating system versions 7](#_Toc147917247)

[7. Security 8](#_Toc147917248)

[7.1. Phones and tablets 8](#_Toc147917249)

[7.2. Windows laptops 8](#_Toc147917250)

[7.3. MacOS Laptops 9](#_Toc147917251)

[7.4. Protection against brute force attacks on devices 9](#_Toc147917252)

[7.5. Other requirements 9](#_Toc147917253)

[7.6. USB devices 10](#_Toc147917254)

[7.7. Stolen or lost personal devices 10](#_Toc147917255)

[8. Duties and responsibilities 10](#_Toc147917256)

[9. Disclaimer 11](#_Toc147917257)

[10. Other applicable policies 11](#_Toc147917258)

[11. Monitoring and review 11](#_Toc147917259)

[12. Approval 12](#_Toc147917260)

# Purpose

This policy covers mobile phones, tablets, and laptops.

Modern devices are capable of accessing and storing data and running business applications. While the use of such devices can bring many benefits, and help staff to better do their jobs, it also introduces a significant risk. That risk is that data, or access to that data, may fall into the wrong hands due to the loss or improper use of the device.

As an organisation we have taken a decision to allow staff to use their own devices such as smart phones, tablets, and laptops for work purposes. This policy has been developed to ensure that this organisation's data is not put at risk from the use of such devices in this manner. For those members of staff with a business requirement to access the organisation’s data with a personal device, this policy provides the necessary guidance so that it is done in a manner that does introduce unacceptable threats to the safety and integrity of this data.

The purpose of this policy is to:

1. Provide effective controls to ensure that staff access to our data and any information systems through the use of devices such as smartphones, tablets and laptops is authorised, secure and confidential, in line with our business requirements.
2. Ensure the remote processing of our data is operated in accordance with statutory requirements and all relevant guidance
3. Ensure that any risks associated with personal device based access are recognised, assessed, and managed.

# Applicability

This policy is applicable to all employees.

# Definitions

**Personal Data:** information that relates to an identified or identifiable individual, as defined by the Data Protection Act 2018 and the GDPR.

**Smart Phones:** A mobile phone that allows users to store information, use email and install programs.

**Tablets:** A portable touchscreen computing device used for accessing and processing data, subject to the organisation's security controls and policies.

**Portable Media Device:** Any portable electronic device capable of storing or transmitting data, including but not limited to USB drives, external hard drives, smartphones, and tablets.

**PDA:** a Personal Digital Assistant or handheld device that combines computing, communication, and organizational features, typically used for accessing and managing data, emails, calendars, and other personal information.

**Laptop:** a portable computing device with a built-in display, keyboard, and storage, designed for personal and professional use.

**User:** Any person authorised to access organisation name's IT systems and networks remotely.

**Encryption:** The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing the key. The result of the process is encrypted information. Password protection is not a form of encryption.

**Bring Your Own Device (BYOD):** The term used to describe the approach of letting members of staff use their own mobile device for work purposes. For example, an organisation might allow their staff to use their own smart phones to access work e-mail while out of the office, rather than supplying corporate owned devices for that specific task.

# Expectation of privacy

Our company will respect the privacy of your personal device and will only request access to the device to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from our corporate policy for company provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using company equipment and/or services.

# Acceptable use

Acceptable use defines standards, procedures, and restrictions for employees who are connecting a personally owned device to our organisation’s network for business purposes. BYOD acceptable use applies to any hardware and related software that is not organizationally owned or supplied but could be used to access organisational resources. That is, devices that employees have acquired for personal use but also wish to use in our business environment.

The overriding goal of this policy is to protect the integrity of employee data and business data that resides within our company’s technology infrastructure. This policy intends to prevent data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to our company’s public image. Therefore, all employees using a personally owned device connected to our organisational network, and/or capable of backing up, storing, or otherwise accessing organizational data of any type, must adhere to our company-defined processes for doing so.

Employees may use their mobile device to access the following resources used by the business:

1. Outlook email
2. Microsoft Teams
3. SharePoint
4. Microsoft One Note
5. Jira
6. Envoy desk booking application
7. Authy authentication application
8. Whatsapp for business group chats

# Devices and support

This section defines the devices and applications covered by our BYOD policy. We expect you to use company laptops and PCs to perform all work-related activities rather than your personal laptop.

The following classifications of media are ones that can be considered:

* Smartphones
* Other mobile phones
* Portable media devices
* PDAs
* Laptops

## Provisioning your device for company use

Please contact our IT team or Office Manager, who will handle the provisioning of your device for business use. To facilitate the provisioning process, we will require the following information:

1. **Device Type:** Specify whether it is a mobile device, USB, tablet, laptop, etc.
2. **Operating System:** Indicate the device's operating system, such as Android, Windows, MacOS, etc.
3. **Current Operating System Version:** Provide the current version of the operating system.
4. **Device Modification Confirmation:** Confirm that the device has not been modified or jailbroken.
5. **Device Locking Mechanism:** Specify the current locking mechanism in use, such as a 6-digit PIN or biometric authentication.
6. **Purpose of Device Usage:** Explain the intended purpose for which the device will be utilised.
7. **Brute Force Attack Measures:** Detail any implemented measures to prevent brute force attacks (refer to section 5.0 for more information).

In rare instances where the device fails to meet our company's security requirements, such as running an outdated operating system or lacking sufficient login protection, it may not be provisioned for business use.

If your device is successfully provisioned, it will be documented in our BYOD asset list, including the provided information. The provisioning will be valid for one year, after which you will need to renew your provision. This one-year expiry ensures that personal devices used for accessing business data and networks do not become outdated and pose potential security risks.

## When do you not need to provision your device

According to the BYOD policy, provisioning your device is not necessary if you solely utilise it for accessing two-factor authentication applications like Authy or for receiving text messages and calls to authenticate your business accounts during login.

## Provision expiry

Due to the rapid advancement of technology and the common practice of replacing smart devices every one to two years, the provision of personal devices is valid for one year only.

To ensure ongoing approval for device usage, employees must apply for a provision extension before the expiration date. It is important to note that if a data breach occurs after the provision has expired and before the extension is approved, the employee will be held liable for any breach and may face disciplinary action.

To initiate the re-application process, please reach out to the IT department and Office Manager.

## Changing personal devices

When transitioning to a new personal device, it is essential that the new device undergoes the provisioning process and is removed from our system before it can connect to the business network.

Additionally, all business applications, data, and login information must be thoroughly erased from the old devices.

## Currently supported operating system versions

To ascertain the suitability of your personal device for work provisioning, it is essential to verify that its current operating system version continues to receive security updates, indicating ongoing support for the device.

All supported versions of Android devices can be viewed here: <https://endoflife.date/android>

All supported Apple smartphone OS can be viewed here: <https://endoflife.date/ios>

All supported Apple iPad OS can be viewed here: <https://endoflife.date/ipad>

All supported macOS can be viewed here: <https://endoflife.date/macos>

All supported Windows OS versions can be viewed here: <https://endoflife.date/windows>

# Security

This section provides an overview of the security measures implemented in our BYOD policy, which outlines the applications and resources accessible to employees through their mobile devices, tablets, laptops, and other devices outlined in this policy. The following are the security requirements we have established.

In order to prevent unauthorised access, devices must be password protected using the features of the device in order to access the company network.

## Phones and tablets

* Employees who wish to use their personal mobile phones and tablets to connect to the business network must comply with one of the following unlocking methods:
	+ A 6-digit PIN code
	+ A 6-character password
	+ Biometric login

**Note:** Combining, for example, a 4-digit PIN and a biometric is now allowed, as it invalidates the security provided by the biometric login.

* Pattern passwords are not allowed on any devices approved for connecting to the company network.

## Windows laptops

If employees use personal laptops running the Windows Operating System, the device unlocking requirements are as follows:

* If the laptop is protected by a PIN code or device-specific password (not tied to a Microsoft account), the code or password must be 6 digits or characters long.
* If the laptop is protected by logging in to a Microsoft account, which is also used for other online services, the password must meet the following criteria:
	+ A minimum length of 8 characters
	+ No maximum length
	+ Avoid using the same password elsewhere or selecting common, easily guessable passwords (e.g., dog's name, date of birth, birthplace, "password12345," etc.).
* If the laptop is protected by biometric login, it should either have no other login options or, if available, the PINs and passwords must adhere to the aforementioned rules.

## MacOS Laptops

If employees use personal laptops running on macOS, then the laptop should be protected as follows:

* If the laptop is protected by a password or a passcode which is not linked to an Apple ID, then it must be at least 6 characters/digits long.
* If the laptop is protected by a password or a passcode which is linked to an Apple ID, then it must adhere to the following criteria:
	+ A minimum length of 8 characters
	+ No maximum length
	+ Avoid using the same password elsewhere or selecting common, easily guessable passwords (e.g., dog's name, date of birth, birthplace, "password12345," etc.).
* If the laptop is protected by biometric login using Touch ID, it should either have no other login options or, if available, the PINs and passwords must adhere to the aforementioned rules.

## Protection against brute force attacks on devices

* Devices must implement measures to protect against brute-force attacks, such as one of the following:
	+ Throttling: Limiting the number of unsuccessful login attempts on the device, allowing a maximum of 10 guesses within 5 minutes.
	+ Locking: Automatically locking the device after 10 unsuccessful login attempts.
* If a device remains idle for five minutes, it must lock itself using previously mentioned methods.

## Other requirements

* Rooted (Android) or jailbroken (iOS) devices are strictly prohibited from accessing the network.
* Only provisioned personal devices are permitted to connect to the business network.
* Users are responsible for ensuring that unauthorised individuals cannot access our data or systems through their enrolled personal devices. When not actively used, provisioned personal device screens, if applicable, should be locked.
* The use of provisioned personal devices for accessing our data or services in public areas should be kept to a minimum due to the risks of information exposure and device theft.
* Personal confidential data must not be stored on unencrypted devices. It's important to note that password protection alone is not a form of encryption and should not be relied upon as such.
* Emails containing personal confidential data and other sensitive information must not be sent to or from personal email accounts.

## USB devices

Personal USB devices should not be used to connect to company issued devices or used on personal provisioned for work devices to transfer company data to it, unless approved by the business in advance.

If the USB device is approved for business use:

* All USB devices must be scanned for viruses and malware before being connected.
* All USB devices containing any business data must be kept securely.
* USB devices should be encrypted, and password protected where possible.

Personal USB devices should not be used to store or transfer any personally identifiable information.

## Stolen or lost personal devices

Lost or stolen devices must be reported to the IT Team and Office Manager within 24 hours who will then follow the data breach procedures in our Data Security Policy.

All accounts used to access the company's network on the device must be accessed using a company-provided laptop, and the passwords for each account must be changed immediately.

If the device has the remote wipe capability, the employee should initiate a remote wipe to erase all data and settings on the device. Remote wiping helps safeguard company data and reduces the risk of data breaches.

In addition to changing their passwords, employees should also review and monitor their business accounts for any suspicious activities. All accounts should have multi-factor authentication enabled, where possible, to add an extra layer of protection to their accounts.

# Duties and responsibilities

**The Data Protection Officer**

The Data Protection Officer (DPO) is responsible for investigating and addressing any data breaches resulting from lost, stolen, or compromised personal devices provisioned for work. The DPO provides guidance to employees and serves as a point of contact for data protection-related matters.

**The IT Department**

The IT Department is responsible for monitoring and responding to data breaches or security incidents related to personal devices provisioned for work. They ensure that all implemented security measures, including technical measures, are appropriate for the business and adhere to the best practices of the National Cyber Security Centre.

**The Office Manager**

The Office Manager is responsible for maintaining an up-to-date asset list of personal devices provisioned for work. This list should be reviewed every 6 months or whenever there are changes, such as new hires or employee departures.

**All Managers**

All managers have the responsibility of ensuring that both current and future staff receive relevant training, guidance, and support to understand and comply with this policy and any associated guidelines.

**All Staff**

All staff members must be aware of their obligations to comply with the requirements for personal device use outlined in this policy. Those with authorized personal devices are responsible for safeguarding company information and promptly reporting any security incidents related to their devices.

# Disclaimer

This section serves as a disclaimer regarding the risks associated with the BYOD policy. Generally, the company shall not be held responsible for any misuse or damages that may occur to a device during its normal operation.

* The employee bears personal liability for all costs associated with their device.
* The employee is expected to consistently use their devices in an ethical manner and comply with the company's acceptable use practices outlined in this policy and other relevant policies.
* The employee accepts full responsibility for risks, including but not limited to, the potential loss of company and personal data due to operating system crashes, errors, bugs, viruses, malware, other software or hardware failures, or programming errors that may render the device inoperable.
* Radcliffe Medical Media Ltd retains the right to take appropriate disciplinary action for noncompliance with this policy.

# Other applicable policies

See our Privacy Policy, Data Security Policy and the Information Security Policy.

# Monitoring and review

The audit of the list of personal devices provisioned for work will take place every 6 months to verify that the operating systems and security requirements continue to meet the expectations outlined in the policy.

Incidents and breaches arising from the use of personal devices provisioned for work will be diligently tracked and documented in accordance with our Data Protection Policy.

The BYOD policy will undergo an annual review to ensure alignment with evolving needs and to address any emerging risks.

# Approval

|  |  |
| --- | --- |
| Name |  |
| Signature |  |
| Approval Date |  |
| Review Date |  |