**Bring Your Own Device Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1.1 | 16/01/2024 | Sultan Mohamed | Nine Taylor | Under review |
|  | June 2025 |  |  | Next review |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 2](#_Toc139517485)

[1.1 Guidance statement 2](#_Toc139517486)

[1.2 Status 2](#_Toc139517487)

[2 Guidance 2](#_Toc139517488)

[2.1 Background 2](#_Toc139517489)

[2.2 Detailed requirements 3](#_Toc139517490)

[2.3 Portable appliance testing (PAT) 4](#_Toc139517491)

[2.4 WhatsApp messaging groups 5](#_Toc139517492)

[2.5 Responsibilities 5](#_Toc139517493)

[3 Summary 5](#_Toc139517494)

[Annex A – Bring Your Own Device User Declaration 6](#_Toc139517495)

# Introduction

## Guidance statement

At this organisation, employees who prefer to use their personally owned IT equipment for work purposes must be explicitly authorised to do so, and must secure the organisation data to the same extent as that on corporate IT equipment. They must not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own equipment.

The owners and users of personally owned devices (PODs) share responsibilities for information security. Nothing in this policy affects this organisation’s ownership of corporate information, including all work-related intellectual property created in the course of work on PODs.

## Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

# Guidance

* 1. **Background**

In contrast to information and communications technology (ICT) devices owned by the organisation, PODs are ICT devices owned by employees or by third parties (such as suppliers, consultancies and maintenance contractors).

PODs are typically:

* Laptops
* Tablet computers
* Ultra-mobile PCs (UMPCs)
* Desktop PCs
* Mobile phones
* Smartphones
* Digital cameras
* Digital memo recorders
* Printers
* Any associated portable storage media such as USB memory sticks, memory cards, portable hard drives, etc.

Authorised employees and third parties may wish to use their PODs for work purposes, for example making and receiving work phone calls and text messages on their own personal mobile phones, using their own computers to access, read and respond to work emails or working in a home-office.

Bring your own device (BYOD) is associated with a number of information security risks such as:

* Loss, disclosure or corruption of corporate data on PODs
* Incidents involving threats to, or the compromise of, the corporate ICT infrastructure and other information assets (e.g., malware infection or hacking)
* Non-compliance with applicable laws, regulations and obligations (e.g., privacy or piracy)
* Intellectual property rights for corporate information created, stored, processed or communicated on PODs in the course of work for the organisation

Due to the organisation’s concerns regarding the information security risks associated with BYOD, individuals who wish to opt-in to BYOD must be authorised by their line manager (with delegated responsibility from the organisation’s SIRO) and must explicitly accept the requirements laid out in this policy before using any PODs.

This organisation reserves the right not to authorise individuals, or to withdraw the authorisation, if they deem BYOD not to be appropriate and in the best interests of the organisation. The organisation will continue to provide its choice of fully owned and managed ICT devices as necessary for work purposes so there is no compulsion for anyone to opt-in to BYOD if they choose not to participate in the scheme.

* 1. **Detailed requirements**

Due to the rapid pace of change it is not possible to support BYOD on all devices. BYOD will only be supported on devices that can run the latest version of the Apple or android operating system. Staff will be expected to make sure their devices are kept updated or risk losing access to some systems.

Devices must be encrypted and have passcode or biometric security if available with a timeout to lock automatically after five minutes of inactivity. Jailbroken or rooted devices are strictly prohibited. Staff must not circumvent security controls.

BYODs should not be utilised for the administration of corporate emails. They must not be used to create, modify, store or communicate corporate data. Should this functionality be required then arrangements should be made with the line manager for the provision of a corporate laptop that will provide appropriate encryption and multi-layer authentication.

Devices may connect over guest or NHS Wi-Fi but are not permitted to connect directly to the corporate network. Staff may only connect to organisation systems for the purpose of authorised work. The use of a device that has access to work systems by BYOD should be limited to its owner and must not be shared. Staff should be conscious of the setting in which devices are being operated and should ensure the data and systems displayed are not visible to others. Data accessed must not be saved to the device or copied off it. **Screenshots of systems must not be taken.**

The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:

* Patient confidential data
* Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as commercially sensitive
* Large quantities of corporate data (i.e., greater than 1 Gb in aggregate on any one POD or storage device)

This organisation has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the POD.

While employees have a reasonable expectation of privacy over their personal information on their own equipment, the organisation’s right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g., “Private” and “BYOD”).

It is important not to infringe other people’s privacy rights, **for example do not use PODs to make audio-visual recordings at work.**

Those wishing to use their own mobile phone POD will need to provide the IMEI number of the device being used and sign an appropriate BYOD declaration (see [Annex A](#_Appendix_A_–)).

* 1. **Portable appliance testing (PAT)**

As with all electrical appliances that are being used within the organisation, any BYOD item must be confirmed to be electrically sound and must undergo PAT in accordance with the [Equipment](https://practiceindex.co.uk/gp/forum/resources/portable-appliance-testing-pat-and-calibration-testing-policy.862/) – portable appliance testing policy.

* 1. **WhatsApp messaging groups**

Whilst the use of WhatsApp groups is acceptable, these should ordinarily only be kept within staffing groups and no messages are to breach the guidance as detailed within the Intranet and Social Media Acceptable Use Policy. Whereas WhatsApp messages should not be used to communicate with patients, this is acceptable when there is no other practical alternative and the benefits outweigh the risk.

Should there be any concerns with any content being messaged, the organisation has the right to seize and forensically examine any POD believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes or on receipt of an appropriate subject access request.

* 1. **Responsibilities**

1. The organisation

Is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the obligations identified in this policy.

An internal audit may be authorised to assess compliance with this policy at any time.

1. The IT Help/Service Desk

Is responsible for providing limited support for BYOD on PODs on a ‘best endeavours’ basis for work-related issues only. Information security incidents affecting PODs used for BYOD should be reported promptly to the practice manager.

1. All employees

Are responsible for complying with this and other corporate policies at all times.

# Summary

To ensure the safety of any data, it is imperative that all staff always follow the guidance within this policy. The organisation will consider revoking the use of PODs for work-related purposes should this guidance not be adhered to.

# Annex A – Bring Your Own Device User Declaration

**BRING YOUR OWN DEVICE USER DECLARATION FORM**

I have been provided with the ability to access Sheerwater Health Centre information and services on my personal computer/device.

In line with the organisation’s policies and codes of practice relating to data protection and information security, it is imperative that any information accessed is safeguarded against loss and inappropriate disclosure to prevent embarrassment to the organisation, a lack of confidence in its working practices and/or a breach of data protection regulations resulting in monetary fine and the imposition of sanctions. In a worst-case scenario, this could result in severe distress or harm to one or more of the organisation’s employees or patients.

I agree that I must:

* Comply with this organisation’s polices and Codes of Practice relating to data protection and information security when using the BYOD application

* Not knowingly download or install any software, programme or utility that undertakes a malicious activity or whose purpose is to alter the security configuration of my computer/device
* Not allow the use of my computer/device to be shared with anyone else whilst logged into the password protected BYOD application
* Inform this organisation’s Information Governance team if my computer/device is misplaced, lost or stolen.

I accept that:

* All charges associated with personal device usage are at the expense of each individual, including any additional call or data charges incurred as a result of using a personal device to access this organisation’s information and services.
* There are no IT support arrangements in place (via the Service Desk)
* This organisation is not liable for any loss of data or functionality as a result of installation
* This organisation is not liable for the loss of or damage to the device

**Declaration**

I confirm I have read and understood this declaration and agree to accept and abide by it. At the discretion of either the partners or management, the [Disciplinary policy and procedure](https://practiceindex.co.uk/gp/forum/resources/disciplinary-policy-and-procedure.746/) may be followed for employees who violate the organisation’s polices and Codes of Practice relating to data protection and information security.

If you are unsure or require clarification about any aspects of the Bring Your Own Device policy, contact your manager or the Information Governance lead.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** |  | **Department** |  |
| **Signature** |  | **Date** |  |
| **Manager’s name** |  | **Department** |  |
| **Signature** |  | **Date** |  |
| **Device** |  | **IMEI Number** |  |
| **Honorarium paid** |  | **Signed off by Practice Manager** |  |

Please forward to the Practice Manager upon completion.