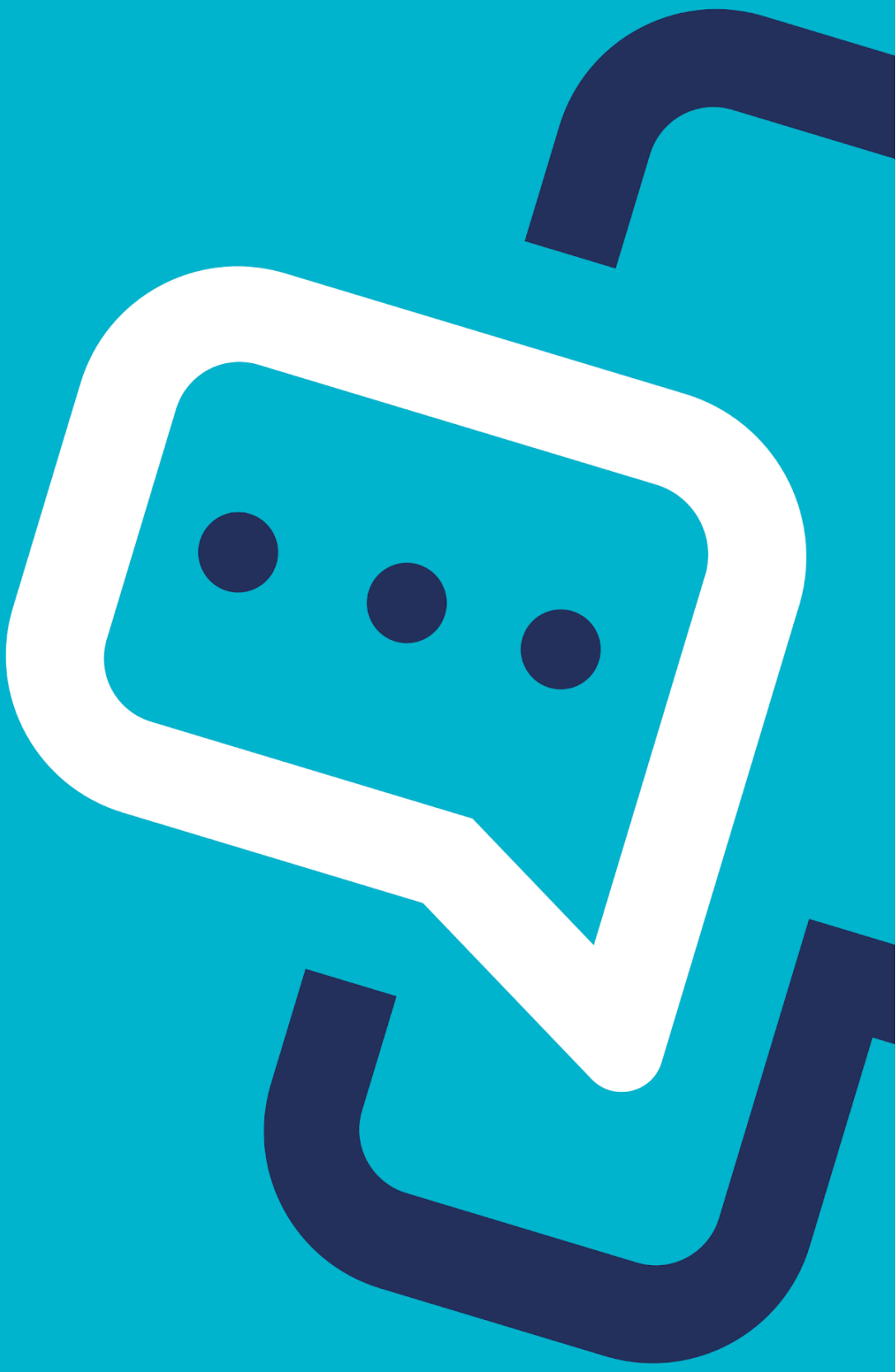
Alertive



Bring Your Own Device (BYOD) Guidance v1.0

Table of Contents

1.Introduction

A BYOD policy is essential for all Trusts that are looking to increase the adoption of mobile devices within their Trust without the capacity, business case or staff support to justify an owned device estate that covers all personnel.

Drafting a suitable policy is difficult as it requires Trusts to balance their duty to protect sensitive patient and other organisational data with respecting the fact that the device is the property of the individual who has privacy and sovereignty rights they may well not wish to surrender.

Installing a mobile device management (MDM) system on the individual's device provides the maximum level of control to the Trust as the MDM operates at device level, and therefore limits the extent that individuals might expose their devices to unauthorised (malicious or accidental) access. However installing an MDM on an individual's device means the user surrenders control of a device which is theirs; which we believe is likely to be strongly opposed.

This could lead to large numbers of users refusing to accept Trust recommended applications and all the problems this brings with it, including:

i) poor adoption levels for mobile-first or enabled applications
ii) use of unapproved alternative applications increasing data security and operational risks
iii) lost opportunities to enhance communication and deliver improved care
iv) requirements to increase the number of Trust-owned devices and associated costs

We have reviewed legal guidance (GDPR, Data Protection Act of 1998, Employment Practices Code), Public sector and NHS guidelines (NHS Confidentiality Code of Practice, NCSC, NHSX suggested BYOD policy), some published BYOD policies (Southern Health NHS Foundation Trust, Ealing CCG) and various corporate BYOD recommendations (Microsoft InTune, VMWare guidance, Jamf and Alertive) to arrive at some suggestions.

This does not constitute legal advice.

2.MDM & MAM (MCM)

There is a distinction between Mobile Device Management (MDM) and Mobile Application Management (MAM) or Mobile Content Management (MCM).

MDM is a client that resides on the device. It provides the highest level of control under BYOD as it enables administrators to take control of management of the device. In the event that this did not significantly impact user experience and user acceptance then this would be the best option. In many cases, and dependent of course on your choice of MDM, it often impacts both significantly.

MAM can operate as a separate client or as part of the application itself. MAM does not control the device itself, which does increase the risk that malware might reside on the device itself as a result of the user accessing peripherals or ill-advised content on the web or held within applications.

MCM is similar to MAM in that it restricts access to organisational information through policies, procedures and technology, but does not go as far as intruding into the operation of the device itself.

3.Legal Requirements

The legal obligations of the Trust are governed by the Data Protection Act 1998 and GDPR.

The Data Protection Act 1998 (DPA) requires that "the data controller must take **appropriate technical and organisational measures** against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

GDPR provides a high level requirement for personal data, that it be "processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The Employment practices code states that employees are entitled to a degree of privacy within the work environment.

Both GDPR and the Data Protection Act 1998 reference appropriate measures but these are not prescribed, so we need to reference various guidelines to determine what these might be.

4.Relevant Guidance

Guidance provides a range of levels of control that might be appropriate. The National Cyber Security Centre (NCSC) suggests that it is critical that administrators should be able to take control of the device itself (ie MDM). Given their primary purpose is to provide guidance on how to combat cybercrime this should be expected as MDM can provide protection in some scenarios that is not possible with MAM or MCM.

NCSC suggests that "logging and audit (are) preferred over prevention and control, to maintain user experience and flexibility for the majority of responsible users", recognising that technology needs to be used to be effective.

NHSX provides guidance on BYOD policies and is less prescriptive. They suggest that "BYOD software" should remain on the device while organisational data is being accessed. They also suggest that organisational policies need to be maintained with BYOD, BYOD devices should be monitored & should maintain the latest version of Apple or Android's operating system.

The ICO's guidance is interesting and probably the most lenient. Some relevant clauses include the following:

i) "It is crucial that the data controller ensures that all processing for personal data which is under his control remains in compliance with the DPA."

ii) "Protecting data in the event of loss or theft of the device will need to be considered but not to the exclusion of other risks."

iii) "Data controllers must also remain mindful of the personal usage of such devices and technical and organisations used to protect personal data must remain proportionate to and justified by real benefits that will be delivered."

Both points ii) and iii) are important overarching concepts for consideration of what level of control is best suited to minimising organisational risk.

5.Technology Vendor Guidance

Many NHS Trusts have access to InTune as part of their Microsoft enterprise licence. Their guidance is as follows:

"For personal devices, or bring-your-own devices (BYOD), users may not want their organization administrators to have full control. In this approach, **give users options.** For example, users enroll their devices if they want full access to your organization resources. Or, if these users only want access to email or Microsoft Teams, then use **app protection policies that require multi-factor authentication (MFA) to use these apps.**"

"As an administrator...configure apps with policies that keep the data protected (such as encrypting it, protecting it with a pin, and so on)... Similar configurations can be deployed for other services and applications that are required by your BYOD users".

6.Published Trust BYOD policies

Ealing CCG suggests that BYOD devices should be protected by MDM.

Southern Health state things differently. They place the onus on the user to support and maintain the device. They reference the GDPR requirement above and believe that MCM tools can be used to ensure controlled access to sensitive information. We have incorporated the items from their checklist in our recommendations below.

7.Proposed Way Forward

We believe that NHS Trusts should create and maintain BYOD policies designed to provide significant protection against any kind of data breach, but that this does not need to be in the form of mandating the use of MDM. There is no legal requirement that MDM be applied and we believe it's unrealistic to expect users to surrender control of their BYOD devices to administrators as this is inconsistent with their personal rights and wishes. We believe that items ii) and iii) above extracted from ICO's guidance support this approach.

In adopting this approach, we need to consider all the protections that are possible and practical under both MAM and MDM and seek to either mitigate or accept these risks.

Should Trusts look to implement MDM on BYOD devices we believe that user adoption will be low and this will result in unapproved communication channels remaining in place, which increases organisational risk, rather than reducing it.

We have outlined our specific policy recommendations below.

8.BYOD Policy Checklist

#	Policy	Source	Satisfied
1	The Trust uses suitable tools to facilitate controlled and secure access to other systems like clinical records	SH	
2	The BYOD security controls must ensure that personal data and trust data are segregated. Policies enforced on a BYOD device are aimed at managing and controlling “Trust” data only.	AL / SH	
3	Any organisational data accessed via an app, must be fully encrypted and any content or attachments saved within a corporate workspace cannot be saved or shared outside the application, except if that application also meets BYOD requirements.	SH	
4	It must be possible to restrict certain user capabilities within the application such as copy and paste, save and view.	MS	
5	All data in transit is fully encrypted	SH	
6	Each of the three types of authentication described here should be considered with at least 2 applied: • User to device: the user is only granted access to the device after successfully authenticating to the device. • User to service: The user is only able to access enterprise services after successfully authenticating to the service, via their device. • Device to service: Only devices which can authenticate to the enterprise are granted access	NCSC	
7	Passwords must be kept safe at all times and should never be shared with other Trust staff or family members. They should meet the requirements of the Trust’s password policies	SH	
8	The Corporate workspace on the device can be remotely wiped if there is cause to believe the device has been compromised. This will only impact the Trust data. The following scenarios should be catered for: -the device is lost -on termination of employment -after 5 failed login attempts -a data or policy breach is detected	SH	
9	IT to perform spot checks to ensure BYOD devices are running the latest operating system.	NHSX	

10	Provide training to staff on the risks that BYOD introduces and how they should help mitigate those risks.	AL	
11	It should be possible to blacklist users even if they maintain live active directory accounts or to restrict their rights to use an application or the capabilities of that application	NCSC	
12	The organisation can access reports on security-critical events and more general data relating to application usage.	NCSC	
13	Your organisation has a plan in place to respond to and understand the impact of security incidents. This should be supported by appropriate functionality within the devices and your organisation. In the case of a lost device, this might entail sending a wipe command to the device and revoking credentials	NCSC	

Tolerated / accepted risks

Risk	Source	Mitigations
An unauthorised entity may be able to modify the boot process of the BYOD device without detection.	NCSC	Staff will be trained on best practices for maintaining the security of their devices. (10) All devices will be Apple or Android and will maintain the latest up-to-date OS containing latest patches (9)
It is not possible to technically ensure that all devices meet security and health requirements eg blocking jailbroken devices	MS	As above
Adherence to the organisational password requirements can't be enforced	AL	The recommended authentication requirements for applications can be technically enforced and are sufficient (6)
You may not be able to see enrolled devices and how organisational resources are accessed.	MS	Devices are not enrolled but organisational access control is required with policies above (12)
The Trust can't define which applications are able to execute on the device, and these policies can't be robustly enforced on the	NCSC	As above

device		

Key:

SH - Southern Health NHS Foundation Trust BYOD policy
MS - Microsoft Intune user guide
NCSC - National Cyber Security Centre guidelines
AL - Alertive recommendations