The NHS Confederation

Charity number 1090329

Company number 04358614

Bring Your Own Device Policy (BYOD)

Date policy agreed by Group Executive:	October 2020
Date of policy review:	October 2022
Owner of policy:	Director of Finance and IT

CONTENTS

Bring Your Own Device (BYOD) Policy

1. Introduction

NHS Confederation provides standard IT equipment for all staff. By default there is no need for individuals to use non-Confed IT equipment but where there is a need to use non-standard equipment, the NHS Confederation will support staff in this practice if they sign up to the terms in this policy and assuming all risks can be managed.

The use of non-standard devices to create and process NHS Confederation information and data creates issues that need to be addressed, particularly in the area of information security.

The NHS Confederation must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. For these reasons use of personal devices may be refused.

2. IT policies

This policy should be read in conjunction with:

- IT Security Policy
- Data protection policy
- Acceptable Use

3. Responsibilities

3.1. Group Executive

The Group Executive is responsible for:

- Approving BYOD users in their business area
- Instructing the IT team to suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full IT access in the event of a breach of policy.

3.2. Staff Members / BYOD users

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of NHS Confederation information (as well as their own information)
- Invoke the relevant security features including:
    - Firewall – turn on Windows defender as a minimum standard
    - up to date anti-virus software
    - Application and operating system must be patched, high and critical patches should be updated within 14 days
    - Passwords and PINs must be in line with NHS Confederations password policy statement within the IT Security Policy.
    - The device must be kept it up to date, at their own cost if applicable.
- Ensure that the device is not used for any purpose that would be at odds with any other NHS Confederation IT or Data Protection policy.
- Ensure the device is not used for illegal activity.
- Ensure that accounts are logged out of when not in use.
- Not access/use the NHS Confederations CRM system. (This should only be accessed/used on a Confed domain joined device)

- In line with the IT Security Policy, ensure that no other person accesses NHS Confederation data or information.
- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of NHS Confederation data and information
- Take responsibility for any software they download onto their device
- Be aware that the IT Team have the right to remotely wipe the device if necessary. This may mean that staff lose personal data.
- Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices. Instead they should use their device to make use of the many services that NHS Confederation offers allowing access to information on services securely over the internet.
- Provide their personal device to IT prior to leaving the organisation or losing ownership of the device, so that IT can check all corporate data has been removed.
- Ensure that relevant information is copied back onto NHS Confederation systems and manage any potential data integrity issues with existing information.
- Report the loss of any device containing NHS Confederation data (including email) to the relevant Director, IT Manager and Head of Governance.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately in line with the Data Protection Policy.
- Not use a device that has had its terms of service broken, such as a 'jailbroken' device.
- Understand that IT retains the right to remote wipe their personal device if it poses a risk to the organisation or its data.

3.3. IT Team

- **The IT team have the right to remotely wipe devices when necessary and this may mean loss of personal data for staff.**
- Will approve BYOD use following receipt of a request form approved by the relevant Director. A copy of the BYOD request form can be found on the Oracle.
- Will review all software installed on the device as part of the setup process.
- Will maintain a list of approved users, and their agreement to abide by this policy when using BYOD.
- Will manage the guidelines and procedures of BYOD in line with this, and any other relevant IT Policies.
- Will ensure that the MDM architecture which supports the BYOD policy is audited on an annual basis to ensure we maintain Cyber Essentials Plus accreditation.
- On request of a Group Executive Director, will suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full IT access in the event of a breach of policy.
- The BYOD requirements are subject to change (sometimes without notice). Any changes to the minimum requirements will be posted on the Oracle by the IT Team.

4. Supporting personal devices

While NHS Confederation IT staff will always endeavour to assist colleagues wherever possible, **NHS Confederation cannot take responsibility for supporting devices it does not provide.** Staff should contact the device manufacturer or their carrier for operating system or hardware-related issues.

5. Monitoring and Access

NHS Confederation will not routinely monitor personal devices. However, the IT team can run audit reports on systems and documents accessed. However, it does reserve the right to:

- Take all necessary and appropriate steps to retrieve information owned by NHS Confederation.
- Prevent access to a particular device from either the wired or wireless networks or both.
- Prevent access to a particular system.

6. Reimbursement of costs for IT equipment

The NHS Confederation will not reimburse the employee for the purchase or associated costs with the device regardless of whether this was incurred for business. This includes, but not limited to roaming charges, plan charges and overcharges, cost of applications for personal use.

Appendix 1 – BYOD request form

Requesting staff member name	
Non-standard equipment to be used	
Why is there a need to use non-standard equipment?	
Supported by Director	
Approved by IT Manager	
Agreed date for set up meeting	

Appendix 2 – BYOD set up checklist

Please note that all of the requirements below must be agreed prior to any connection to the NHS Confederation systems.

Requirement	Agreed (Yes or No)	Initials of employee
The mobile device remains your responsibility – NHS Confederation will not undertake fix / maintenance / replacement of your device.		
NHS Confederation has the right to wipe the device		
NHS Confederation will take no responsibility for the loss / removal of any personal data held on the device associated with the operation of security on the device.		
If you lose your device then you must inform NHS Confederation immediately – if this is outside of operational hours, then on the next working day.		
Provide your personal device to IT prior to leaving the organisation or losing ownership of the device, so that IT can check all corporate data has been removed.		
Antivirus is installed and must be kept up to date		
Password check		IT Team Initials
Software check		IT Team Initials
The device must be included in the BYOD asset list.		IT Team Initials

Employee Declaration

I _____ have read and understood the Bring Your Own Device Policy and consent to adhere to the rules outlined.

I understand this is in addition to any other policy of the NHS Confederation.

Employee name	
Employee signature	
Date	

IT team name	
IT team signature	
Date	