# Consumer Device Policy (Smartphones / Tablets)

| Policy Number: | 422 | Supersedes: | - | Classification | Corporate |
|---|---|---|---|---|---|

| Version No | Date of EqIA: | Approved by: | Date of Approval: | Date made Active: | Review Date: |
|---|---|---|---|---|---|
| V1 | 28/04/2015 | IGC | 28/04/2015 | 28/04/2015 | 28/02/2018 |
| V2 | N/A | BPPAC | 28/08/2018 | 13/09/2018 | 28/08/2021 |

| | |
|---|---|
| Brief Summary of Document: | The policy relates to any staff member (or manages a staff member) who uses the Choose Your Own Device (CYOD) or Bring Your Own Device (BYOD) scheme in Hywel Dda University Health Board. |
| Scope: | All staff that are part of the scheme or manage staff that are part of the scheme needs to adhere to this policy (i.e. users of smartphones and tablets for Health Board business). |
| To be read in conjunction with: | 183 - Information Security Policy<br>281 - Mobile Working Policy<br>280 - Email Policy<br>108 - Internet Access and Usage Policy |

| | |
|---|---|
| Owning Committee | Information Governance Sub-Committee |

| Executive Director: | Karen Miles | Job Title | Director of Planning, Performance and Commissioning |
|---|---|---|---|

| Reviews and updates | | |
|---|---|---|
| Version no: | Summary of Amendments: | Date Approved: |
| 1 | New Policy | 28/04/2015 |
| 2 | Updated | 28/08/2018 |

Glossary of terms

| **Term** | **Definition** |
|---|---|
| MDM | Mobile Device Management, software that provides features that enables a device to be used in a secure manner. |
| BYOD | Bring Your Own Device |
| COYD | Choose Your Own Device |
| GDPR | General Data Protection Regulations |
| ICT | Information & Communication Technologies |
| Jail Broken | Apple device that has been modified to install apps and make configuration changes not authorised by Apple. |
| Rooted | Andriod device where access has been given to modify the software on the device to make unauthorised changes. |
| WPAS | Welsh Patient Administration System (formally Myrddin CiS). |

| | |
|---|---|
| Keywords | Information, Informatics, Mobile Working, BYOD, CYOD, Tablet, Smartphone, IT, ICT, Apple, Andriod |

## CONTENTS

## 1. Introduction

The Health Board has the goal to enable greater flexibility to allow the use of Smartphones and Tablets to access health board data and applications. These could be both corporately owned devices (Choose Your Own Device – CYOD) and personally owned devices (Bring Your Own Device – BYOD).

This policy will therefore use the terms BYOD and CYOD throughout and are clarified below:-

- BYOD – refers to Bring Your Own Device and is the scenario where a health board employee chooses to use their own smartphone or tablet to access health board information and systems.
- CYOD – refers to Choose Your Own Device and is the scenario where the health board has purchased a smartphone or tablet for the use by the employee whilst undertaking Health Board business.

This will allow you to access:-

- Your work email
- Your work calendar
- Your work contacts
- A secure work web browser (Access to internal web sites)
- Access to internal file stores
- Citrix based applications
- Public applications available in App Stores which maybe of relevant to your role
- Private applications which might be developed in the future by Hywel Dda and/or its partners.

The use of portable devices and mobile platforms is now commonplace in our personal lives and this consumerisation of IT is now spreading into NHS use. For many years‟ laptops and blackberry devices have been used to provide remote access to information but the adoption of tablets and smartphones has the potential to deliver many benefits to health board staff especially those which are mobile.

This mobile device use however poses a substantial risk in that devices may be lost, damaged, or stolen, potentially resulting in loss or inappropriate disclosure of data. When using mobile devices, the risks of working in an unprotected environment must be considered and mitigated where possible by the use of appropriate security systems and the procedures outlined in this policy.

**It is noted that some staff may use their own device for work business outside of this scheme, all staff are reminded that it is not permitted to use consumer applications such as WhatsApp, Dropbox and Snapchat etc. for the transfer of Person Identifiable Information (PII) or confidential Health Board information. These activities could result in a breach of the Data Protection Act / General Data Protection Regulations or any subsequent legislation to the same effect and enforcement activities against the Health Board and disciplinary procedures against the individual.**

## 2. Policy Statement

To utilise any of these services to access corporate data and applications, all users of the service will agree to the following terms and conditions before ICT can enable the service. This will be communicated in writing over email and a record retained.

All users of this service will fully comply with corporate policies on appropriate mobile phone, e-mail and internet usage. These can be found on the intranet.

All users of the service must familiarise themselves with the corporate information governance policies and ensure they are adhered to.

- All users of this service will need to adhere to the security policies of the health board ensuring safe access to corporate data and applications.
- A security application will provide the health board with the ability to lock down and secure the device such as enforcing a password and encrypting the device.
- Policies enforced on your device are aimed at managing corporate data and applications, your personal information on BYOD devices will not be affected.
- Policies on CYOD which are corporately owned will be aimed at managing the device and whilst personal information can be stored on these devices it is done so at your own risk and ICT will not be able to recover any personal information lost.
- You will keep your password / passcode secret and not allow anybody else to access the information. This will be setup when the device is first registered and will need to be changed at periodic intervals.
- Should you lose or have your BYOD device stolen you will need to report this to ICT immediately so that we can remove corporate data from it remotely. It will be the user's responsibility to report the theft of the device to the authorities.
- Should you lose or have your CYOD device stolen you will need to report this to ICT immediately so that we can wipe the device remotely. The health board will then report the theft of the device to the relevant individuals in the health board.
- In the unlikely event that personal data on the BYOD device is affected or lost, HDUHB will not be held responsible or liable for any damages or compensation. Any personal data on the CYOD device will be lost if the device is stolen or lost as the device will be wiped completely.
- You will inform the HDUHB ICT department if you no longer need access to these services and we will remove the app from your device and retire it from the service.
- You accept that the HDUHB will not be liable for any charges relating to the handset hardware, tariff, insurance, call or data charges incurred when using BYOD devices.
- You understand the app might interfere with the operation of your phone / tablet and accept this; examples include enforcing a lock screen passcode / password and encryption.
- You accept that the HDUHB offers no support or maintenance for the phone/tablet and it is your responsibility to maintain or repair it as and when required for BYOD devices. CYOD will be fully supported by the Informatics Service Desk.
- No cloud services should be used to store health board data such as Apple's iCloud, GoogleDrive, Dropbox and Microsoft OneDrive. Separate services are available to enable data to be shared with third parties or for home access. Please contact the Informatics Service Desk to access these.

**Failure to adhere to these protocols will result in the withdrawal of the service.**

## 3. Scope

All staff that are part of the scheme or manage staff that are part of the scheme needs to adhere to this policy.

## 4. Aim

The aims of this policy are:

- To ensure that the Health Board complies with its legal obligations against the General Data Protection Regulations (2016) and Data Protection Act (2018), or any subsequent legislation to the same effect.
- To promote the safe and secure use of mobile equipment in support of the clinical and operational work of Hywel Dda University Health Board.
- To provide a secure working environment for personnel working remotely on corporate / public wireless networks and 3G/4G mobile connections.
- To ensure that resources provided to staff are not misused.
- To ensure that the security of mobile systems and the information they contain is not compromised in any way.

The policy applies to all full-time and part-time employees of the Health Board, Independent Members, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement with Hywel Dda University.

## 5. Objectives

Mobile working must be authorised and controlled by heads of departments / budget holders.

The Health Board's approved method of enabling the required security is the mobile device management product called MobileIron. The user needs to input their Cymru username and password which ensures strong authentication.

Users will be required to sign a declaration before access is granted.

Mobile phones and similar devices used for application / data access must have a security PIN number, passcode enabled, or biometric security such as fingerprint / facial recognition.

Patient identifiable information (PII) or other confidential Health Board data must not be stored permanently on mobile devices or media. Where possible information should be transferred to the Health Board's secure network and deleted from the device as soon as possible.

All devices will be enrolled onto the system using the vendor's current enterprise deployment method such as Apple Deployment Enrolment Programme or Andriod Enterprise.

## 6. Service Policy

### 6.1 Applying for the Service

There will be a cost for this service which is viewable on the Informatics Intranet Site. Your manager will need to approve this spend and provide ICT with a cost code.

Please log a call with the Informatics service desk or use the online form to access the service.

### 6.2 Acceptable Use

- The Health Board defines acceptable business use as activities that directly or indirectly support the services within HDUHB.
- Acceptable use for Internet and E-mail use is available in the relevant existing policies.
- For BYOD the Health Board defines acceptable personal use on company time as reasonable and limited personal communication.
- Devices" camera and/or video capabilities will not be disabled but must be used within the relevant health board guidelines for handling images.
- CYOD devices may not be used at any time to:-
    - Store or transmit illicit materials.

- Harass others.
- Engage in outside business activities.

- A white list of applications will be maintained and these maybe pushed directly to the device on registration.
- CYOD will have policies applied to ensure a blacklist of applications are maintained so that these cannot be used on health board devices.
- Employees may use their mobile device to access the following Health Board resources: email, calendars, contacts, documents, websites and approved applications.
- HDUHB has a zero-tolerance policy for texting or emailing while driving.

6.3 Devices and Support

- Smartphone's including iPhone, Android, Blackberry and Windows phones are allowed and a detailed list will be maintained on the Intranet.
- Tablets including iPad, Windows and Android are allowed and a detailed list will be maintained on the Intranet.
- Connectivity issues are supported by ICT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues for BYOD devices.
- The BYOD software supports Android devices but due to the various implementations of the Andriod operating system by manufacturers we cannot guarantee all devices will function as required.
- NO "jail broken" or rooted devices are allowed and will be automatically rejected and will not connect to the service.

After a licence is purchased and a user account is setup on the system you will be sent instructions on how to add your device to the service.

- The "work" space is a secure container which enables access to your work email, calendar, contacts and a secure web browser. There will also be a work app store where we recommend certain public applications that we feel are useful applications and any apps that have been developed for Hywel Dda.
- Email – you will have access to work email and lookup users from the directory.
- Tasks – These are sync'd with our email system.
- Calender – These are sync'd with our email system.
- Secure web browser – this will allow access to work web sites e.g. the intranet.
- Access to work files and the ability to create docs (subject to pending Office 365 implementation).
- Please note there are limitations with the degree of functionality of internal applications. This relates to how the application has been designed to function in a traditional PC/Laptop environment with larger screens. If you still wish to access web applications (such as the Welsh Clinical Portal) or applications via Citrix (HDDAPPS) such as WPAS, you can do but in the knowledge that full functionality may not be available and navigation may be difficult.

## 7. Responsibilities

7.1 Reimbursement

- The Health Board will not reimburse the employee for a percentage of the cost of the BYOD device.
- The Health Board will not reimburse the employee for data changes on BYOD devices.

7.2 Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and your Cymru password is required to access the Health Board wireless network.
- Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password cannot be one of 15 previous passwords.
- The device will lock itself with a pass code or PIN if it's idle for five minutes.
- After five failed login attempts, the device will lock. Contact ICT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the service.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on Health Boards list of approved apps on CYOD devices.
- For CYOD the device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) ICT detects a data or policy breach, a virus or similar threat to the security of the Health Boards data and technology infrastructure.
- For BYOD the secure container will be wiped removing health board data and applications, personal data will not be affected.

7.3 Data Security

The work space area is fully encrypted whilst on the device and all data in transit to and from the device is fully encrypted. The device integrity and authenticity is continually checked for any security risks and immediately blocked if detected.

The work space is protected with a password / PIN and it is your responsibility to keep this safe and we would recommend that you make this memorable and complex. Should you lose the device or you feel the work area could be compromised you must inform the Informatics Service Desk immediately and we will wipe the work area. This will NOT interfere with any personal data of the device for BYOD devices. If you forget your workspace password after 10 attempts it will delete the work space and all work data within it. ICT do not have sight of the password and cannot recover it

7.4 Risk / Liabilities / Disclaimers

- The Health Board can accept no liability for the loss of any private information held on a BYOD or CYOD device such as documents and photos.
- While ICT will take every precaution to prevent the employees personal data from being lost in the event it must remote wipe the secure container, it is the employee's responsibility to take additional precautions, such as backing up your personal device using the iCloud for example.
- The health board reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the Health Board immediately. Employees are responsible for notifying their mobile carrier immediately upon loss of a BYOD device. A self-service portal will also be available for employees to disable their own devices if required.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Health Boards acceptable use policy.
- The employee is personally liable for all costs associated with his or her BYOD device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors,

bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

- HDUHB reserves the right to take appropriate disciplinary action for noncompliance with this policy.

## 8. Roles & Responsibilities

8.1 Directors

Directors are responsible for the management of information risk within their control and in particular are responsible for ensuring their staff are aware of the information risks identified within this policy and take responsible action to mitigate them.

Directors must:-

- Ensure procedures are in place within their sphere of responsibility to enable the identification and assessment of information risks of mobile computing and the implementation of control measures, including staff training and awareness to mitigate the risks.
- Ensure all mobile and teleworkers are appropriately approved and authorised. This should include a procedure to ensure that mobile computing and removable media devices used are approved for Health Board equipment that has been encrypted.

8.2 Line Managers

Managers are responsible for ensuring that all their staff have read and understood this policy prior to authorising mobile computing arrangements. They must ensure that staff work in compliance with this policy and other appropriate legislation and Health Board policies. This includes the responsibility for ensuring that risk assessments are or have been carried out and that suitable controls are put in place and remain in place to either eradicate or minimise any identified risks to the security of Health Board information.

Line managers **must** inform the Informatics Service Desk when a member of staff leaves the Health Board or changes role.

8.3 All Staff

All staff, whether permanent, temporary or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality and understand they are required to comply with this policy. Failure to comply with this policy may result in disciplinary action being taken, which may result in the withdrawal of authorisation and the service.
Staff shall inform their manager if they have any concerns about any issues that would constitute an information risk. This covers not only risks to resources or confidentiality of data, but also personal risk, risk to others and risk to the Health Boards reputation.

Staff need to confirm to their line manager that they understand this policy and their responsibility for the protection and security of the Health Board information they access.

Health Board information must only be used for Health Board related purposes in connection with Health Board work.

Staff are responsible for ensuring that unauthorised individuals are not able to see any confidential Health Board information or access Health Board systems.

Users of information will:-

- Keep usage to a minimum in public areas.
- Only use information off-site/at home for work related purposes.
- Ensure security of information within the home.
- Not send patient identifiable or confidential data to home (internet) e-mail addresses.

8.4 ICT Department

- Fulfil requests to access the scheme.
- Provide advice and direction on the use of this scheme.
- Ensure adequate security controls are implemented in support of this policy.
- Provide reports on usage of the scheme and retire inactive devices from the service.