Reference Number: UHB 423 **Version Number:** 1.1	**Date of Next Review:** 8th Aug 2020 **Previous Trust/LHB Reference Number:** N/A

BRING YOUR OWN DEVICE (BOYD) LOCAL PROCEDURE

Introduction and Aim

This document is written in support of the Information Technology (IT) Security Policy and the NHS Wales All Wales Policies. It provides a mechanism to achieve and maintain appropriate security arrangements in respect of Cardiff and Vale University Health Board's (the UHB) IT systems that hold confidential and sensitive patient and business information.

The IT Security procedures of the UHB are to ensure the safety and security of all UHB IT systems, software and in particular the UHB's Network so as to produce a safe and secure environment in line with NHS and statutory policies and procedures. This document provides further information as to the detail of the policy and its supporting information.

Objectives

- Successful implementation of this procedure will address business and performance standards for example the requirement to meet Caldicott standards, Health and Care Standards (2015)
- Aspire to meeting BS7799/ISO27001 standards and the Information Governance Toolkit Standards as far as possible in the Welsh context.

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts

Equality Impact Assessment	An Equality Impact Assessment has been completed for the overarching IG and IT Policies. The assessment found that there was some impact on the equality groups mentioned in relation to communication. An action plan has been developed to address those areas.
Health Impact Assessment	A Health Impact Assessment (HIA) has not been completed. Not Required.
Documents to read alongside this Procedure	Information Governance Policy Information Technology Security Policy Information Risk Management Procedure A Guide to Incident Reporting NHS Wales All Wales Internet Use Policy
Approved by	Information Governance Sub Committee
Accountable Executive	

or Clinical Board Director	
Author(s)	Richard Williams (IT Security) Ann Morgan (Information Governance)

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	08/08/17	28/08/18	List title and reference number of any documents that may be superseded
1.1	08/08/17	28/08/18	Version updated to reflect current contact details

Contents Page

1 Introduction

The UHB has the goal to enable greater flexibility by allowing the use of personally owned devices, referred to as '*Bring Your Own Device*' (BYOD), such as smartphones and tablets to access the UHB data and applications

The '*Blackberry Good*' service utilised by the UHB allows staff access on their own device to:

- work e-mail
- work calendar
- work contacts
- secure work web browser (access to internal web sites)
- Citrix based applications
- Public applications available in App Stores which maybe of relevant to work role
- Private applications which might be developed in the future by the UHB IM&T IT Developments and/or its partners
- work office documents (such as Microsoft Word and Excel)

The use of portable devices and mobile platforms has been commonplace for a considerable time via laptops and Blackberry devices to provide remote access to information, however the adoption of smartphones and tablets has the potential to deliver many benefits to UHB staff especially those who are frequently mobile

The service provision by '*Blackberry Good'* provides a secure working 'bubble' environment for security, whereby no data is stored on the mobile device. The use of smartphones and tablets 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 conformity requirements as outlined in this document

For an video overview of '*Blackberry Good*' visit Blackberry Apps Info page on the UHB intranet (http://helpdesk/help/BlackberryDynamicsIntro_B.html)

2 Responsibilities

The UHB

The UHB is not responsible for the liability or reimbursement to UHB staff for:

- a percentage of the cost of their BYOD device
- data charges on their BYOD devices

- any damages or compensation in the unlikely event that personal data on their BYOD device is affected or lost

The UHB reserves the right to take appropriate disciplinary action for noncompliance with this procedure

Department Managers
Department Managers are responsible for:

- The management of information risk within their control
- Ensuring their staff are aware of the information risks identified with mobile communication
- Staff training and awareness to mitigate the risks identified
- All mobile staff are appropriately approved and authorised at a department management level for use of mobile devices
- Provision of a valid cost code with the mobile working order request to the IT Helpdesk for licensing and setup costs, as appropriate. The cost for this service can be viewed on the UHB intranet (http://helpdesk, select option 'Install or Upgrade Software', then option 'Home & Mobile Working Services')

Line Managers
Managers are responsible for ensuring that:

- All their staff have read and understood this procedure prior to department management authorising mobile computing arrangement
- Staff work in compliance with this procedure and other appropriate legislation and UHB 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 the UHB information

IT Services Department
The IT Helpdesk can be contacted to provide the following information:

- A list of supported smartphones and tablets
  The '*Blackberry Good***'** application does support Android but due to the various implementations of the Android operating system by manufacturers the UHB cannot guarantee all devices will function as required

The IT Helpdesk is responsible for providing the following services:

- Upon receipt of order for '*Blackberry Good*' and valid cost code, a licence is purchased and a user account is authorised on the system. The new user being sent instructions on how to add the service to the BYOD device
- Support for '*Blackberry Good*' connectivity issues
  However BYOD end-users should contact the device manufacturer or their carrier for operating system or hardware-related issues for BYOD devices

BYOD staff users

To utilise the '*Blackberry Good*' services for access to UHB corporate data and applications, all users of the service must agree to the following terms and conditions before IT Services can enable the service

All BOYD staff users of this service:

- Will fully comply with the UHB corporate policies on appropriate mobile phone, email and internet usage, these can be found on the intranet
- Must familiarise themselves with the corporate Information Governance policies and ensure they are adhered to
- Will need to adhere to the security policies of the UHB ensuring safe access to corporate data and applications
- Policies enforced on BOYD devices are aimed at managing corporate data and applications, personal information on BYOD devices will not be affected
- 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 the UHB IT Helpdesk immediately so that potential remote access to corporate data can be suspended. It will be the user's responsibility to report the theft of the device to the police for an incident number
- In the unlikely event that personal data on the BYOD device is affected or lost, the UHB will not be held responsible or liable for any damages or compensation
- You will inform the UHB IT Helpdesk if you no longer need access to these services, who will retire your access from the service
- You accept that the UHB will not be liable for any charges relating to the smartphone/tablet hardware, tariff, insurance, call or data charges incurred when using BYOD devices
- You accept that the UHB offers no support or maintenance for the smartphone/tablet and it is your responsibility to maintain or repair it as and when required for BYOD devices
- No cloud services should be used to store UHB data such as Apple's iCloud, Google Drive, Dropbox and Microsoft OneDrive. Separate services are available to enable data to be shared with third parties or for home access. Please contact the UHB IT Security Manager to access these
- In order to prevent unauthorized access, devices must be password protected using both the features of the BOYD device and the '*Blackberry Good*' application
- You are expected to use BYOD devices in an ethical manner at all times and adhere to the UHB's acceptable use as summarised below
- Ensure unauthorised individuals are not able to see any confidential UHB information or access UHB 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 person identifiable or confidential data to home (internet) e-mail addresses
- Not dispose of any media (including paper) off-site

Failure to adhere to these responsibilities will result in the withdrawal of the service

3 Acceptable Usage

The UHB defines acceptable business use as activities that directly or indirectly support the services within the UHB that are within the following parameters:

- Acceptable use for Internet and Email use is available in the relevant existing All Wales and local policies
- The UHB defines acceptable personal use on the organisations time as reasonable and limited personal communication
- Devices' camera and/or video capabilities will not be disabled but must be used within the relevant UHB guidelines for handling images
- Staff may use their mobile device to access the following UHB resources: email, calendars, contacts, documents, intranet, internet websites and approved applications
- The UHB has a zero-tolerance policy for texting or emailing while driving

---

This document is one of several that sustain the UHB's IT Security Policy and IT Security Procedure

Useful Contacts

Appendix 1

IM&T IT Security cv.imt.security@wales.nhs.uk

Head of IT and Strategic Planning
Nigel Lewis Nigel.Lewis@wales.nhs.uk
Tel 02920 745600

Technical Development, Network and Support Manager
Gareth Bulpin Gareth.Bulpin@wales.nhs.uk
Tel: 02920 745605

IT Security Manager
Richard Williams richardt.williams@wales.nhs.uk
Tel 02920 745608

IT Helpdesks
UHW (East) IT.Helpdesk.UHW@wales.nhs.uk
Tel 02920 745073
UHL (West) Llandough.Helpdesk@wales.nhs.uk
Tel 02920 715218

Information Governance cav.ig.dept@wales.nhs.uk
Including Data Protection/Freedom of Information and E-mail monitoring

Senior Manager, Performance and Compliance
Paul Rothwell paul.rothwell@wales.nhs.uk
Tel 02920 743677

Corporate Governance Senior Information and Communication Manager
Ann Morgan ann.morgan4@wales.nhs.uk
Tel 02920 744870

Information Governance Officer
Vanessa Clement-Pugh Vanessa.celement-pugh@wales.nhs.uk
02920 745624

Information Governance Co-ordinator
Denise Gulley denise.gulley@wales.nhs.uk
02920 745625