INFORMATION GOVERNANCE SUB-COMMITTEE COMMITTEE UPDATE REPORT

Date of last meeting: 26 November 2025

Quoracy: Unmet 26 November 2025

Report by: Anthony Tracey, Digital Director, Chair

KEY DISCUSSION POINTS AND MATTERS TO BE ESCALATED FROM THE DISCUSSION AT THE MEETING:

Alert (may require discussion)

Information Governance Sub-Committee wishes to **alert** members of the Digital, Data and Innovation Committee that:

- Although Information Governance training compliance is above 85%, some departments still require improvement, which will be addressed through the Mandatory Training Group.

Advise (to monitor)

Information Governance Sub-Committee wishes to **advise** members of the Digital, Data and Innovation Committee that:

- Due to IGSC not being quorate, the Sub-Committee scrutinised extensions to the All-Wales IG policies (listed below) and also Health Board for DDIC to approve:
  - 836 - All Wales Information Governance Policy
  - 837 - All Wales Information Security Policy
  - 494 - All Wales Email Use Policy
  - 495 - All Wales Internet Usage Policy
  - 282 - Network Security Policy
  - 319 - Disposal of Digital Assets Policy
  - 422 - Consumer Device Policy

Assure (to note)

Information Governance Sub-Committee wishes to **assure** members of the Digital, Data and Innovation Committee.

- Compliance with Information Governance training has risen from 77% to 85.3%, marking the first time the Health Board has successfully achieved the national benchmark.

Review of Risks

The Sub-Committee reviewed the risks which are aligned to them. As part of its review, the Sub-Committee considered the status of each risk, and the current score was deemed in tolerance.

Sharing of learning

Not applicable

Recommendation

The Committee is asked to:

- **APPROVE** the extensions to the All-Wales IG policies (836,837,494 and 495).
- **APPROVE**; 282 Network Security Policy, 319 Disposal of Digital Assets Policy and 422 Consumer Device Policy.
- **NOTE** the items that the Committee is advising them of.
- **TAKE ASSURANCE** from the items that the Committee is assuring them of.

Network Security Policy

Policy information

Policy number: 282
Classification: Corporate
Supersedes: Previous versions
Version number: 4.0 Draft
Date of Equality Impact Assessment:

Approval information

Approved by:
Date of approval:
Date made active:
Review date:

Summary of document:
This policy states the network security requirements for the Health Board

Scope:
This policy applies to all users of the Health Board's digital networks.

To be read in conjunction with:
837 - AW Information Security Policy – opens in a new tab
201 – AW Disciplinary Policy – opens in a new tab
281 – Mobile working policy – opens in a new tab

Patient information:

Owning group:
Information Governance Sub-Committee Click or tap to enter a date.

Executive Director job title:
Director of Finance

Reviews and updates:
1 – new policy 26.6.2012
2 – revised 29.3.2016
3 – full review 28.2.2023

Keywords
Network, security, access, computing

Glossary of terms
None

Keypoints:
To ensure the security, integrity and availability of the Health Board's digital networks used to support our clinical and administrative services.

Contents

INTRODUCTION

This document defines the computer network security policy for Hywel Dda University Health Board and this policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

It sets out the policy for the protection of the confidentiality, integrity, and availability of the network as well as security responsibilities for ensuring the security of our networks.

The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected using our local and wide area networks.

POLICY STATEMENT

The overall Network Security Policy for the Health Board is described below.

The Health Board's information network will be available when needed, can be accessed only by legitimate users and devices, and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this the Health Board will undertake the following: -

- Protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.
- Where relevant comply with the legal, regulatory, and internal policy requirements.

If a user is found to have breached this policy, they may be subject to the Health Board's disciplinary procedure. – opens in a new tab.

If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from the Health Board's Network or Cyber Security Team.

SCOPE

This policy applies to all networks within Hywel Dda Health Board both wired and wireless used for: -

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending, and storing non-clinical or clinical data or images

AIMS

The aim of this policy is to provide assurance through relevant controls and procedures that our networks are secure and the information on them is kept confidential.

OBJECTIVES

The objectives to be achieved by this policy are: -

- Suitable controls exist to secure our networks.
- Ensure all those accessing and managing the network understand their roles and responsibilities.
- Ensure suitable procedures are in place.

Risk Assessments

Hywel Dda University Health Board will carry out security risk assessment(s) in relation to all aspects of the network that are used to support business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.

Formal risk assessments will be conducted in line with Health Boards Risk Assurance Framework.

Physical and Environmental Security

The following Physical and Environmental security mechanisms will be employed: -

- Network computer equipment will be housed in a controlled and secure environment that is monitored for temperature, humidity, and power supply issues.
- Critical network equipment will be housed in dedicated secure areas protected by physical locks and access control mechanisms.
- The Head of Digital Operations is responsible for ensuring the suitability of these security measures.
- Network equipment will be protected from power supply failures.
- Critical network equipment will be protected by intruder alarms and fire suppression systems.
- Various technical controls will be in place to secure the network including security patching, firewalls, and network admission control.
- All visitors to secure and critical network areas must be authorised by the Head of Digital Infrastructure.
- The Head of Digital Infrastructure will ensure that all relevant digital employees are made aware of procedures for visitors and those visitors are escorted when necessary.

Access Control to the Network

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. Ordinarily, such access is supervised but there may be occasions when trusted engineers may require unsupervised access. The Head of Digital Infrastructure will maintain and periodically review a list of those with unsupervised access. Access to these areas will be restricted by appropriate controls.

Access to the network will be via secure methods and authentication against our directory service. Remote access to the network will conform to the Health Board's Mobile Working Policy – opens in a new tab.

There must be a formal, documented user registration and de-registration procedure for access to the network. All users on the network will have their own individual user identification and password and are ensuring their password is kept confidential. Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working and workstations must be locked if a workstation is left unattended.

User access rights will be immediately removed or reviewed for those users who have left the Health Board or changed jobs.

Any device connecting to the corporate network must comply with the Health Board's Managed security requirements which include domain membership, Endpoint Detection and Response, Secure Web Gateway, and patching procedures. Devices that do not meet these requirements are not permitted to connect to the corporate network.

Clinical devices and Internet of Things (IoT) equipment connecting to the network must be placed in a segregated virtual network to ensure they are protected from the wider network and have controlled access control lists.

Requests for New Devices to Access the Network

Any department that has a need to connect new IoT or IoMT corporate devices to the corporate network must request formally via the Digital Services portal, Device Connectivity Request. The Cyber Security Team will need to review any new devices prior to connection. Departments must request this before procuring any new devices to ensure they meet the Health Boards security standards. Any devices that are procured without Digital Services approval may require significant network re-configuration to ensure they can be added securely which will incur additional costs.

Third Party Access to the Network

If external third-party owned devices require access to the corporate network this will be allowed only once the third party has provided assurances of their security posture of the organisation and device to the cyber security team where possible the free public and patient guest Wi-Fi service should be used ("Hywel Dda Public").

All third-party access to the corporate network must be logged and access to Hywel Dda Health Board's systems must be always audited.

Third party users must have an Active Directory account created for them for the duration of their stay with appropriate permissions and will not use generic accounts or service accounts.

Any department that has a need to connect new third-party owned devices to the corporate network must request formally via the Digital Services portal, Device Connectivity Request.

All third remote access by external third parties must be approved following the Code of Connection process and must utilise Hywel Dda approved remote access methods.

Physical access by 3rd parties to network equipment locations (Server Rooms, Communication Rooms, Cabinets etc) must be approved by Digital Services. 3rd parties must be supervised when physically working in these areas to maintain system security.

Network Monitoring

The Hywel Dda corporate network is monitored by an Armis network discovery tool. This monitors all devices connected to the network and provides a status of the device's vulnerabilities. New devices that are connected to the network are automatically reported to the Cyber Team via Armis. If a formal request to connect the device has not been received prior to connection, the Cyber Team reserve the right to block the device until an appropriate security review has been conducted.

External Network Connections

Any external network connections must only be through approved access methodologies and managed by the Digital Services department to ensure they can be appropriately secured and monitored.

Any connections not formally approved my put the Health Board at risk by disconnection from the Public Sector Broadband Aggregated Network (PSBA)

Personally Owned Devices

Under no circumstances should personally owned devices be connected to the corporate network. This includes plugging them into any network sockets located on walls throughout the estate, or attempting to connect them to corporate Wi-Fis (i.e. Hywel Dda or Hywel Dda Corporate).

Personally owned devices are only permitted to be connected to the available guests Wi-Fi networks available through the estates (i.e. _Hywel Dda Public)

Maintenance Agreements

The Head of Digital Operations will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Digital Department's Configuration Management Database.

Operating Procedures

Documented Security Operating Procedures will be created for the network that reflects this policy and changes to these procedures must be authorised by the Head of Digital Infrastructure.

Change Control

Any changes proposed to the network must consider the security of the network.

Changes must be in line with the Hywel Dda change control procedure and must be reviewed by the Digital Change Advisory Board and approved by the Head of Digital Infrastructure.

As part of acceptance testing of all new network systems the Cyber Security Manager will undertake security tests to ensure compliance with this policy.

Security Monitoring

The network will be monitored for potential security breaches and automated alerts will be generated to highlight potential issues.

All potential security breaches must be reported to the Cyber Security Team using the Digital Portal. The Cyber Security Manager is responsible for auditing the network to ensure it meets agreed security standards.

RESPONSIBILITIES

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are: -

Users

The health Board will ensure that all users of the network are provided with the necessary security guidance, awareness, and where appropriate training to discharge their security responsibilities.

All users of the network must be made aware of the contents and implications of the network security policy and that irresponsible or improper actions by users may result in disciplinary actions(s).

All users should safeguard hardware, software and information in their care and prevent the introduction of malicious software onto the organisation's digital systems.

They also have an obligation to report on any suspected or actual breaches in security.

Digital Operations

Digital Operations will be responsible for: -

Management of our network equipmentManage our network security including that of the Wireless LAN and any external connections not a part of the PSBA network.

- Be responsible for Disaster Recovery and Business Continuity Plans and for the testing of those plans.
- Provide support to users in gaining access to the network and their use of services provided over the network.
- Periodic penetration testing to ensure the security of our networks.

Head of Digital Operations

Will be responsible for implementing an effective framework for the management of network security and ensure the production of all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of this policy.

Head of Digital Infrastructure

Will be responsible for the implementation of effective security countermeasures contacting the Cyber Security Manager when incidents or alerts have been reported that may affect the security of the Health Board's networks.

Responsible for ensuring all network components will have effective configuration management procedures in place in line with the Hywel Dda Configuration Management Procedure.

Cyber Security Manager

The Cyber Security Manager will be responsible for: -

- Will be responsible for the mandating of effective security countermeasures.
- Acting as a central point of contact for cyber security within the organisation.
- Assisting in the updating of this policy and related policies for approval by the Information Governance Sub-Committee.
- Produce organisational standards, procedures, and guidance on cyber security matters.
- Liaise with external organisations on cyber security matters, including representing the organisation on the national Operational Security Service Management Board and associated sub-groups managed by Digital Health & Care Wales (DHCW).
- Advising the Head of Digital Operations on cyber security breaches and recommended actions.
- Encouraging, monitoring, and checking compliance with this policy.
- Promoting awareness and providing guidance on this policy.
- Creating, maintaining, and giving guidance on and overseeing the implementation of network security.

Line Manager's Responsibilities
Ensuring all employees are made aware of their security responsibilities as indicated in this policy.

TRAINING

All staff will be required to have appropriate information governance training which will include guidance on network security.

IMPLEMENTATION

All staff must adhere to this policy and failure to follow these policies may lead to disciplinary action being taken. This policy will be disseminated through global email and through periodic Information Governance training.

Disposal of Digital Assets Policy

Policy information

Policy number: 319
Classification: Corporate
Supersedes: Previous versions
Version number: 4
Date of Equality Impact Assessment:

Approval information

Approved by:
Date of approval:
Date made active:
Review date:

Summary of document:
The purpose of this policy is to outline the steps that need to be taken to ensure that all digital equipment is disposed of in the appropriate manner in terms of confidentiality and Waste Electrical and Electronic Equipment (WEEE) legislation and regulations.

Scope:
This policy covers the disposal of all digital equipment in particular the disposal of any computer related equipment computer media, audio tapes and removable media.

The policy applies to all materials which contain confidential information for example: paper records, photographs, computer media and audio tapes

To be read in conjunction with:

183 - Information Security Policy – opens in new tab
275 - Secure Transfer of Personal Information – opens in new tab
494 - All Wales E-mail Policy – opens in new tab
281 - Mobile Working Policy – opens in new tab
282 - ICT Security Policy – opens in new tab

Patient information:
Not applicable
Owning group: IGSC

Executive Director job title: Director of Finance

Reviews and updates:
1 – new policy 28.1.2023
2 – revised policy 26.6.2018
3 – revised policy 28.2.2023

Keywords
Information, Personal Data, Personal Information, Informatics, Transfer of Information, Mobile Working, Screensaver, Information Technology, Acceptable Use Equipment, Information Asset, ICT Asset, Digital

Glossary of terms
ICT – Information and Communication Technology
PC – Personal Computer
WEEE – Waste Electrical and Electronic Equipment
PAT – Portable Appliance Test
Health Board – Hywel Dda University Health Board

Contents

Introduction

The Health Board has a duty of care to ensure that the disposal of digital equipment, especially those with disks or removable media containing information and data is undertaken with due care and attention. If any files contain personal or other sensitive or confidential data, then special care must be taken to ensure that this information cannot be accessed by anyone. There have been high profile cases where this care has not been adequately exercised; the Data Protection Act/General Data Protection Regulations 2018 or any subsequent legislation to the same effect requires that these issues are given serious consideration.

In addition, there are obligations that must be met for any person receiving the equipment in relation to its electrical safety that may represent a continuing liability or environmental implications in disposing of computer equipment.

Scope

This policy covers the disposal of digital equipment, in particular: -

- The disposal of any computer related equipment. This includes Servers, connected medical devices Personal Computers (desktop or laptop), mobile devices (tablets, smartphones), mobile phones, printers, scanners, and any other peripheral devices such as memory sticks.
- The policy applies to all materials which contain confidential information for example computer media and audio tapes.

This policy links to the Health Boards policies covering - Confidentiality, Data Protection, Records Management, and Information Security. Together these policies form an integral part of the Health Boards approach to Information Governance and Cyber Security.

Aim

The aim of this policy is to outline the steps that need to be taken to ensure that all digital equipment is disposed of in the appropriate manner in terms of confidentiality and Waste Electrical and Electronic Equipment (WEEE) legislation and regulations.

Objectives

The aims of this policy will be achieved through: -

- Effective communication with Health Board employees so they are aware of the procedures to follow.
- Digital department procedures to cover the effective disposal of equipment.

Definitions

Hardware

By its own nature digital equipment is constantly evolving and this can therefore become a very broad category making it impossible to list every single item or group of items within this policy document; however physical assets can be summarised as follows: -

- Desktop Devices
    - PC or Workstation
    - A Laptop, Tablet Computer or digital mobile device including Apple and Android devices
    - Telephones
- Data Centre Components
    - Servers, Storage systems, Power Distribution Units
    - Backup Devices, Backup appliances, Magnetic Tapes
- Local or standalone Devices
    - Printer, Scanner. Multi Function Device (MFD)
    - Security equipment (e.g. CCTV, Door Entry system)
- Network attached equipment
    - Printers, Scanners, MFDs
    - Medical Devices
    - Network Switches, Routers, Firewalls
    - Security equipment (e.g. CCTV, Door Entry systems)
    - Access Control systems such as card swipe systems
- Mobile devices (Cellular / WiFi connections)
    - Smart Phone
    - Smart Tablet
    - DECT Phones and their infrastructure equipment
    - Cellular infrastructure equipment
    - WiFi infrastructure equipment

Software

Providing a complete list of applications used by Hywel Dda University Health Board is not feasible, and detailing all acceptable uses for each application would be an extensive process. However, the software can be summarised as follows. : -

- Desktop Software – all applications and related data loaded onto a Desktop or Laptop computer.
- Server Software – all applications and related data loaded onto a server.
- Hosted Solution – all applications and related data (owned by the Health Board) hosted off site either in the National Data Centres or in a third-party provided Data Centres.
- Software as a Service – all applications and related data hosted in public cloud services such as Microsoft Azure and Amazon Web Services.

Electronic Data

Electronic Data can be summarised as follows: -

- CD’s / DVD’s
- Backup Tapes
- Memory Sticks
- Videos

Disposal of Digital Equipment Procedure

The Digital Operations department will assess whether equipment is redundant for its original use. This will be following discussion with the system owner and/or departmental manager. The disposal of Digital equipment procedures will cover all Health Board Equipment.

Equipment Disposal

Upon request an assessment will be made on the equipment by digital operations staff. Where possible equipment will be redeployed throughout the Health Board or offered to other NHS Wales organisations via the WarpIT portal.

Regardless of the path the equipment has taken there are only three reasons for disposing of equipment, they are as follows: -

- Redundant (fully functioning / not functioning)
- Broken (reasons known / reasons unknown)
- End of Life / Support and hence a Cyber Security Risk

Generally, Digital equipment will reach its natural end of life when it is between five and seven years old, however there are likely to be some exceptional circumstances where equipment becomes redundant mid-term due to specific machines (PCs and Laptops) needing to run specialised software where the specification of the machines has been exceeded.

In all instances an assessment (triage) must be undertaken to determine the validity of disposal of the equipment and to ensure authorisation is granted for the removal of the equipment from the asset system.

Where equipment is determined to be redundant an assessment will be made to determine whether the equipment can be used for digital inclusion.

Redundant Equipment

This is equipment that is no longer fit for purpose and is incapable of running the standard software deployed at the time. Typically, this will be the equipment that is five years of age or older. Redundant equipment that is not working will be disposed.

Broken Equipment

This is equipment that is not working and is out of warranty. Broken equipment that cannot be repaired will be disposed. It is also possible that broken equipment that can be repaired will be disposed when the cost of repair is greater than, equal to or just less than the cost of replacement. It may also be where the cost of repair is financially inappropriate, such as equipment which is nearing five years old is therefore due to be replaced soon.

End of Life

This is equipment which may be functioning correctly but has reached its end of life and is no longer supported by the manufacturer. Such equipment may no longer receive security updates or pose a risk to the Digital Operations of the Health Board. In such circumstances the equipment may be disposed of and replaced as required from available funds.

Disposal Method

In all instances all Health Board owned equipment will disposed via the Digital Services approved scheme.

However, for redundant functioning equipment owned by the Health Board, it would be appropriate for this equipment to be reused in another suitable scenario or broken down as spares for other units that may yet have a small element of life within them. If no spares can be claimed from the unit, then it will disposed.

Under absolutely no circumstances can any computer equipment be directly sold (or given) to any individual or other organisation. The procedure contained within Appendix A must be followed for all equipment and under no circumstances should any computer equipment be disposed of via undesignated skips, recycling centres or landfill.

All equipment disposals will be undertaken within current and future Waste Electrical Equipment (WEEE) legislation. However, Digital Services reserves the right to review this arrangement, with prior notification, as more equipment falls within the WEEE directive.

When re-deploying equipment, the Digital Operations Department will, if required, arrange for all equipment that does not have an up-to-date Portable Appliance Test (PAT) certificate to be tested prior to redeployment by the Estates Department.

Digital Inclusion

Where equipment is determined to be redundant an assessment will be made to determine whether the equipment can be used to support the Health Board's digital inclusion agenda. If so, the equipment will be securely wiped and provided for use by the digital inclusion team in our local communities to help improve digital accessibility and digital skills.

Media Destruction

Media, which is no longer required (or has passed its effective reuse period), should be dealt with as outlined below.

All media including CD-ROM's, DVD's, Hard Drives, USB memory keys and tapes will be dealt with by the Digital Services approved scheme and will be shredded and therefore destroyed using industry standard equipment.

Incidents

It is the responsibility of ward / department / unit managers to report incidents. Advice and guidance regarding confidential waste or record storage can be sought from the Head of Medical Records.

The Health Boards Risk Incident Reporting Procedures, DATIX, and security incidents must be followed, and the investigation / action accurately documented.

Responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are.

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

Executive Directors must: -

- Ensure procedures are in place within their sphere of responsibility to enable the identification and assessment of risks, including staff training and awareness to mitigate the risks.

Digital Services
Digital Services are responsible for: -

- For assessing whether the equipment could be suitably redeployed in another department or used for digital inclusion.
- Before disposal Digital Services will confirm with the user that no data is held locally which needs to be retained.
- In the event of such data being discovered then the data will be copied for safe storage and security onto network file storage.
- The equipment maybe dismantled and used for spare part purposes. In this case the hard disk will be erased to a complete and unrecoverable state.
- If any equipment is un-repairable or has no other useful life it will be disposed of, and the hard disk will be physically destroyed.
- After disposal Digital Services will record disposal on the relevant asset register, including the reason and method of disposal and which technician undertook the task.
- Physical disposal of assets must adhere to WEEE Regulations and ensure that disposal is both secure and environmentally responsible.

Line Managers
Managers are responsible for ensuring that all their staff have read and understood this policy. They must ensure that staff work in compliance with this policy and other appropriate legislation and Health Board policies.

Inform the Digital Service Desk of any digital equipment which require disposal.

All Staff
All staff, 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.

Staff must: -

- 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.

- Be responsible for ensuring that unauthorised individuals are not able to see any confidential Health Board information or access Health Board systems.
- Should staff become aware that a breach of confidential information has taken place the Health Boards Information Governance incident response process should be followed immediately.

Consumer Device Policy
(Smartphones / Tablets)

Policy information

Policy number: 422
Classification: Corporate
Supersedes: Previous versions
Version number: 4
Date of Equality Impact Assessment:

Approval information

Sustainable Resources Committee
Date of approval:
Date made active:
Review date:

Summary of document:
This policy defines the roles and responsibilities, objectives and policy statements relating to the use of smart phones or tablets to access Hywel Dda University Health Board (Health Board) data or IT systems.

Scope:
The policy relates to any staff member (or manages a staff member) who uses a Health Board corporate smartphone or tablet, or their own smartphone or tablet to access Health Board IT services.

To be read in conjunction with:
837 – All Wales Information Security Policy – opens in a new tab
281 - Mobile Working Policy – opens in a new tab
494 – All Email Policy – opens in a new tab
495 – All Wales Internet Access and Usage Policy – opens in a new tab
320 – Acceptable use of information and communication technology policy – opens in a new tab

Owning group: IGSC

Executive Director job title: Director of Finance

Reviews and updates:
1 – new policy 28.4.2015
2 – updated 28.08.2018
3 – full review 28.2.2023

4- updated 27.10.2025

Keywords
Information, Digital, Mobile Working, COBE, BYOD, Tablet, Smartphone, IT, ICT, Apple, Andriod

Glossary of terms

MDM	Mobile Device Management, software that provides features that enables a device to be used in a secure manner.
COBE	Corporate Owned Business Only, corporate issued devices that must only be used for business purposes.
BYOD	Bring 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	Android device where access has been given to modify the software on the device to make unauthorised changes.
WPAS	Welsh Patient Administration System.
Health Board	Hywel Dda University Health Board

Contents

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 (Corporate Owned, Business Only - COBE) and personally owned devices (Bring Your Own Device – BYOD).

This policy will therefore use the terms BYOD and COBE 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.
- COBE – refers to Corporate Owned Business Only 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. These devices should only be used for business use only.

This will allow you to access: -

- Your work emails
- Your work calendars
- Your work contacts
- A secure work web browser (Access to internal web sites)
- Access to OneDrive
- Microsoft Teams
- Other O365 applications (e.g. Viva Engage)
- 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 during the pandemic the use of these technologies in the NHS has grown considerably. 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 using 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.

Policy Statement

To utilise any of these services to access corporate data and applications, all users of the service will need to understand the following terms and conditions. There is no registration required for the BYOD scheme and it is available to all staff once they have setup Microsoft Multi-Factor Authentication (MFA).

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 Health Board's Intranet or Internet site.

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

- All staff will need to register for Microsoft Multi-Factor authentication and either use the app on the smartphone / tablet, receive SMS messages or automated phone calls.
- 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 on COBE devices. No applications are installed on personal devices using the BYOD scheme.
- Policies enforced on your device are aimed at managing corporate data and applications, your personal information on COBE devices will not be affected.
- Policies on COBE 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 digital 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. Where possible use biometric authentication such as your thumb print where the device supports this.
- Should you lose or have your BYOD device stolen you will need to report this to Digital immediately so that we can revoke access to corporate data remotely. It will be the user's responsibility to report the theft of the device to the authorities.
- Should you lose or have your COBE device stolen you will need to report this to digital 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, the Health Board will not be held responsible or liable for any damages or compensation. Any personal data on the COBE device will be lost if the device is stolen or lost as the device will be wiped completely.
- You accept that the Health Board will not be liable for any charges relating to the handset hardware, tariff, insurance, call, or data charges incurred when using BYOD devices.
- You accept that the Health Board 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. COBE will be fully supported by the Digital Service Desk.
- No cloud services should be used to store health board data such as Apple's iCloud, GoogleDrive and Dropbox. Separate services are available to enable data to be shared with third parties or for home access. Please contact the Digital Service Desk to access these.
- Under no circumstances should PII data relating to patients be stored directly onto devices. Data should remain in the relevant application and service for that data. Ie WPAS/ WCP etc.

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

Scope

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

Aim

The aims of this policy are:

- To ensure that the Health Board complies with its legal obligations against the Data Protection Act including UK GDPR (2018) and the Network & Information System Regulations (2018).
- 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 4G/5G 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.

Objectives

The Health Board's approved method of enabling the required security is through Microsoft Intune which is part of the Microsoft 365 suite of productivity tools.

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 systems 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 Android Enterprise.

Service Policy

Applying for the Service

Please use the online form to access the COBE scheme. Your manager will need to approve this spend and provide Digital with a cost code.

All users have automatic access to the BYOD scheme and it is personal preference whether a member of staff chooses to use or not.

Acceptable Use

- The Health Board defines acceptable business use as activities that directly or indirectly support the services within the Health Board.
- 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. Policies will ensure Health Board data cannot be shared outside of corporate apps such as Outlook.
- COBE devices may not be used at any time to: -
    - Store or transmit illicit materials.
    - Harass others, particularly on the grounds of any protected characteristic as defined in the Equality Act 2010.
    - Engage in outside business activities.
- A list of applications will be maintained and these maybe pushed directly to the device on registration.
- COBE will have policies applied to ensure a disallow list of applications and internet sites are maintained so that these cannot be used on health board devices.
- Employees may use their own mobile device to access the following Health Board resources: email, calendars, contacts, documents, websites, Microsoft 365 applications and other approved applications.
- The Health Board has a zero-tolerance policy for texting or emailing while driving.
- Staff must not allow unauthorised individuals access to Corporate systems and data via their COBE and BYOD.

Working Abroad

- Calls on Hywel Dda mobile phones are blocked by default outside of the UK. Requests to use a Health Board mobile phone outside of the UK should be submitted to the IT Service Desk at least 10 days before travel. Each request will be reviewed on a case-by-case basis. Users are required to keep call and data to a minimum to perform business function, to keep charging costs as low as possible.

Devices and Support

- Smartphones including iPhone and Android are allowed to use this service.
- Tablets including iPad, Windows and Android are allowed to use this service.
- Health Board app issues are supported by Digital Services; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues for BYOD devices.
- 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.

- Microsoft Outlook
    - Email – you will have access to work email and lookup users from the directory.
    - Calender – access to your work appointments
- Task Management
    - Microsoft To Do and Microsoft Planner

- Microsoft Teams
- Secure web browser (Microsoft Edge) – this will allow access to work SharePoint sites e.g., the Intranet.
- Access to work files and the ability to create docs (using Word, PowerPoint, Excel etc.).
- 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 applications via Citrix (HDDVAPPS) such as WPAS, you can do but in the knowledge that full functionality may not be available and navigation may be difficult.

Responsibilities

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.

Security

- For BOYD devices the following is employed:
    - conditional access policies are in place to protect Health Board data
    - staff must use Microsoft Authenticator to access Health Board data
- For COBE devices the following is employed:
    - To prevent unauthorized access, devices must be password protected using the features of the device.
    - The device will lock itself if it's idle for five minutes.
    - After 11 failed login attempts, the device will lock. Contact the Digital Service Desk to regain access.
    - The minimum password length is 6 characters and must be complex.
    - Password expiry is 90 days.
    - Internet protection
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the service and are blocked by default.
- Employees are automatically prevented from downloading, installing, and using any app that does not appear on Health Boards list of approved apps on COBE devices
- For COBE 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 users account will be removed from the license group therefore removing access to health board data and applications, personal data will not be affected.

Data Security

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

Should you lose your device, or you must inform the Digital Service Desk immediately and we will remove access. This will NOT interfere with any personal data of the device for BYOD devices. If you forget your password after 10 attempts, it will delete the corporate device and all work data within it. Digital Services do not have sight of the password and cannot recover it

Risk / Liabilities / Disclaimers

- The Health Board can accept no liability for the loss of any private information held on a BYOD or COBE device such as documents and photos.
- While Digital Services will take every precaution to prevent the employee's personal data from being lost it is the employees 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 always use his or her devices in an ethical manner and adhere to the Health Boards 320 - acceptable use policy. – opens in a new tab.
- 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.
- The Health board reserves the right to take appropriate disciplinary action for noncompliance with this policy.

Roles & Responsibilities

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.

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 Digital Service Desk when a member of staff leaves the Health Board or changes role.

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.

Digital Services
- 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.