INFORMATION GOVERNANCE SUB-COMMITTEE COMMITTEE UPDATE REPORT

Date of last meeting: 5 June 2025

Quoracy: Met

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 wish to **alert** members of the Digital, Data and Innovation Committee that:

- **Mobile Working Policy (281)** – the Sub-Committee approved the updates changes to the policy (see Appendix 1)
- **All Wales Policies Extension** – the Sub-Committee approved the extension for the following All Wales Policies –
    - 836 – All Wales Information Governance.
    - 837 – All Wales Information Security Policy
    - 495 – All Wales Internet Usages Policy
    - 494 – All Wales Email Use Policy

Advise (to monitor)

The Information Governance Sub-Committee had no matters of which to **advise** members of the Digital, Data and Innovation Committee.

Assure (to note)

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

- **Information Governance Annual Report 2024-25** - The Sub-Committee received and approved the Information Governance Annual Report. Members expressed their appreciation to all contributing colleagues for their valuable insights and dedicated efforts throughout the year.

Review of Risks

The two risks which are aligned The Sub-Committee were reviewed. 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 Mobile Working Policy (281)

- **RESPOND** to the items that the Committee is alerting them to
- **TAKE ASSURANCE** from the actions that the Sub-Committee is providing assurance on.

Mobile Working Policy

Policy information

Policy number: 281

Classification:
Corporate

Supersedes:
Previous Versions

Version number:
4.0 (Draft)

Date of Equality Impact Assessment:
02/10/2023

Approval information

Approved by: Sustainable Resources Committee (SRC)
Date of approval:
Click or tap to enter a date.
Date made active:
Click or tap to enter a date.
Review date:
Click or tap to enter a date.

Summary of document:
The policy relates to any staff member, who at any time removes records and other information in any form, from Health Board owned premises, where it is usually stored in a secure manner.

Scope:
The policy relates to any staff member, who at any time removes or records information in any form, from Health Board owned premises, where it is usually stored.

The authorisation procedure only relates to staff that need to use mobile computing facilities, either on or off-site (including staff homes), or transfer information between computer systems via physical media.

The policy applies to all full-time and part-time employees of the Health Board, non-executive directors, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement with Hywel Dda University Health Board, volunteers and staff of partner organisations with approved access.

To be read in conjunction with:
837 - All Wales Information Security Policy (opens in a new tab)
422 - Consumer Device Policy (Smartphones / Tablets) (opens in a new tab)

Patient information:
Include links to Patient Information Library

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

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1.0 – New Policy
2.0 – Revised
3.0 – Full Review
4.0 – Blocked countries section included

Keywords
Information, Personal Data, Personal Information, Informatics, Transfer of Information, Mobile Working

Glossary of terms
IAO - Information Asset Owner
NHS – National Health Service
NWIS - NHS Wales Informatics Service
PID - Person Identifiable Data
BYOD - Bring Your Own Device
ICT – Information and Communication Technology
PC – Personal Computer
SIRO – Senior Information Risk Owner
UK – United Kingdom

Contents

Introduction

The use of portable devices and mobile computing equipment is now commonplace in the NHS with users connecting remotely to required information services through laptops, home computers, smartphones, and tablets. Users are also connecting from a variety of locations – home, hotels, NHS, and council premises, and through broadband and wireless technologies.

The use of mobile working when accessing digital services has increased significantly during the COVID 19 pandemic with many staff now working regularly from home or using new digital tools in community settings.

Mobile computing 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 computing, the risks of working in an unprotected environment must be considered and mitigated where possible by the use of appropriate security procedures or facilities which the digital team will implement. The ability to work remotely using Office 365 tools (such as E-mail and Microsoft Teams) is now available for all staff.

Policy statement

This policy has been developed to promote best practice with regards to information handling outside the boundaries of the Health Board premises (including working at home).

The policy is aimed at enabling and supporting employees who intend to use and transfer manual and electronic person identifiable records between home, the workplace and the community.

The Heath Board's Policy is that remote access to the network will be subject to robust authentication using two-factor authentication for authorised users which ensures that data is encrypted during transit across the Internet.

The Health Board's approved method of remote connections is below

- Microsoft 365 for access to E-mail, Microsoft Teams and office applications such as Microsoft Word.
- Cisco Anyconnect which is available on Health Board laptops
- Citrix Access Gateway which is available on work and personal devices for applications available on our Citrix platform.

For all the methods above the user needs to register for Microsoft Authenticator which provides two-factor authentication and their existing Cymru username and password. Microsoft Authenticator can either be used with a smartphone app, text message or automated callback.

Health Board owned mobile devices and media must be encrypted and any sensitive data sent to or from that device should be encrypted during transit.

Person identifiable data (PID), 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 or applications and deleted from the device as soon as possible.

Unauthorised software must not be installed onto Health Board mobile devices. Anti-virus scanning will be installed and regularly updated.

Scope

The policy relates to any staff member, who at any time removes or records information in any form, from Health Board owned premises, where it is usually stored.

The policy applies to all full-time and part-time employees of the Health Board, non-executive directors, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement with Hywel Dda University Health Board, volunteers, and staff of partner organisations with approved access.

Aim

The aim of this document is to:

- To ensure that the Health Board complies with its legal obligations.
- 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 practice for personnel working from home.
- To ensure that resources provided to staff are not misused.
- To ensure that the security of computer systems and the information they contain is not compromised in any way.

Objectives

The aim of this document will be achieved by the following objectives:

- As the use of mobile computing resources grows it is vital that the data held on these devices is not compromised by poor security practises. Mobile devices are by their very nature vulnerable to being both mislaid as well as being attractive to a potential criminal. It is important therefore that all users of mobile equipment such as: laptop computers, tablets, smartphones and mobile storage devices (‘memory sticks’) are aware of the inherent risks associated with their use.
- It is now mandatory that all laptop computers are encrypted to the Health Board’s required security standards before use. In addition, all mobile phones need to have an initial password to help prevent unauthorised access to the device and any user who wants to use Bring Your Own Device (BYOD) or have a corporate Smartphone will be protected by the Health Board’s mobile device management solution. If you are unsure if your equipment has the necessary security applied to it, please contact the Digital Service Desk for advice and assurance.
- All staff using mobile computing equipment or working offsite are required to comply with this policy. Failure to do so may result in this facility being removed or disciplinary action being taken against individuals.

Physical Security / Access Control

Usage in any Publicly Accessible Area

The use of information in these areas should be kept to an absolute minimum, due to the threats of “overlooking” and theft. Any member of staff choosing to use information and/or devices in these areas that results in any related incident will be required to state why the usage was required in that situation and the efforts they made to protect the information and any equipment. Equipment in use should not be left unattended at any time.

Home Usage
All staff can access digital services at home using the methods outlined in the policy statement however only authorised members of staff are allowed access to Health Board information being used at home in paper format. No family members are allowed access to the equipment or data.

Use of any information at home must be for authorised work purposes only.

Staff must ensure the security of information within their home from theft as well as ensuring that unauthorised individuals are not able to see information or access systems. Where possible any paper records should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored away.

Supplied Equipment
Where the Health Board has supplied any form of computing device, only the member of staff themselves is authorised to have access to it or another Health Board employee.

Any member of staff allowing access to an unauthorised person, deliberately or inadvertently, may be subject to disciplinary proceedings.

If staff have been supplied with mobile equipment (i.e., a laptop or similar device), they are responsible for ensuring that it is connected to the Health Board's network via Cisco Anyconnect for implementation of security patching at least once a month. All anti-virus updates are delivered over the Internet and do not require connection to the Health Board's network.

All Health Board mobile devices or removable media must be encrypted before any information is stored.

When equipment is returned, or the data is no longer needed the data must be removed. This is the user's responsibility.

Staff Owned Equipment
The use and storage of person identifiable or confidential data on staff owned equipment is strictly forbidden. Staff may only use a Health Board supplied encrypted USB memory key for this purpose or use the Citrix secure remote access service / Microsoft Office 365 with Microsoft Authenticator.

For prevention of viruses and related security risks, staff must not connect any personally owned devices to the Health Board network and instead use the free Public / Guest Wi-Fi which is available across the organisation.

Mobile Computing

It is important to take all reasonable steps to ensure that any mobile computer device is not misplaced or stolen. This should include leaving it out of sight when away from the workplace, particularly when travelling in a car when it should be locked in the boot. In busy areas such as bus stops, railway stations, it should not be placed on the ground, beside you on a counter, or left unattended at any time.

In the home environment any computer system is vulnerable to theft. To reduce this, devices should where possible be located so that they are not visible through windows from outside the home. Laptops, Tablets and Smartphones in particular must be placed in a secure location when not in use.

All mobile computer devices and removable storage devices should be encrypted by Digital Services before use.

Internal Network Connections
Only Hywel Dda owned or managed equipment is to be connected to the Health Board's network, this includes all mobile computing devices including Laptops, Tablets, encrypted memory sticks, audio, photographic and video equipment etc.

The free guest and patient Wi-Fi service is available to use where wireless coverage exists.

External Network Connections
Remote access to Hywel Dda network **must** be via the Health Board's approved solutions which provides two-factor authentication. Where remote access tokens are being used (currently being phased out) they should not be carried in the same bag as the device to which they provide access.

Staff must ensure that they do not download any attachments to their home pc. They must also ensure that Health Board information cannot be accessed or viewed by members of their family/visitors.

The computer must never be left unattended whilst access is open to the Health Board network.

Staff who have a need to use a mobile computing device to work on Health Board information offsite and have been given line manager authority, are required to comply with the following:

- The equipment must be encrypted.
- The device should be afforded all reasonable protection at all times and especially whilst mobile and located away from Health Board.
- Mobile devices must not be left unattended where it can be seen and open to theft.
- The authorised user will be held responsible for the correct operation of the device and for all data processing and storage.

Software Security Measures

All data is to be stored/and or synchronised to a Hywel Dda network or other approved secure storage system (such as Microsoft Office 365) to ensure that it is backed up daily or when mobile working permits.

Person Identifiable or confidential information is **not** to be stored on to or copied to any removable storage device unless this is appropriately encrypted to the correct security requirements. (E.g., encrypted data stick/flash drive). In certain circumstances it may be necessary to seek the permission of the relevant Information Asset Owner (IAO) to hold such data in this format and if in doubt please seek their advice/approval.

In circumstances where there is a clear business case and the IAO consent has been given, such data may be stored on the mobile computer equipment or removable storage device providing they meet the criteria of this policy.

All data which has been approved for storage on the mobile device is to be copied to an appropriate network drive, or other approved secure storage device, as soon as practicable to ensure that data is backed up.

Printing

The Health Board does not provide printers, nor does it support access to home printers any printing required to undertake roles should be printed at work prior to working from home. This should not include employee or commercially sensitive or patient identifiable information. Any paper must be disposed of securely in adherence to Health Board policy. Employees must not print and take-home paper documents of sensitive/confidential nature or patient data unless this has been approved by Head of Service and Information Governance and an appropriate risk assessment has been completed.

Blocked Countries

To reduce the risk from Cyber threats, devices that try to use Hywel Dda UHB or NHS Wales services from high-risk countries have been blocked. Hywel Dda UHB or NHS Wales IT services will not be available to both personal or corporate devices in these countries.

A list of blocked countries can be found in this article.

If you are required to use or access IT services while in blocked countries, you must request a temporary exemption through the IT Services Portal.

Exemption requests must be submitted at least 10 working days before travel.

Responsibilities

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

Chief Executive

The Chief Executive has overall responsibility for all written control documentation within the Health Board.

Digital Services Department

The Digital Services Department are responsible for:

- Ensure procedures are in place within their sphere of responsibility to enable the identification and assessment of information risks of mobile computing and remote working and the implementation of control measures to mitigate the risks.
- That all necessary security controls have been implemented and configured.
- Undertake regular audits to ensure:
    - All users are approved, that all mobile devices issued can be accounted for and that assurance can be given to the SIRO that identified risks are adequately controlled and managed.
    - Equipment holding Health Board data is an information asset and must be recorded on the Digital asset register.

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. 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.

All Staff

All staff, whether permanent, temporary or contracted, should 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. If staff are unable to comply with this policy, they should discuss in the first instance with their line manager.

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 Board's reputation. Wilful failure to comply will be addressed via separate policies.

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. Agreement on how staff will comply with this policy when working away from Health Board controlled premises, should be reached with their line manager.

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

Staff are not permitted to hold person identifiable data or any other Health Board sensitive data on personally owned equipment, in particular home PCs although they can access data using one of the approved methods outlined in the policy statement. Holding other commercially or business sensitive Health Board data on personal equipment would breach Health Board policies concerning information security and records management.

Staff must not, under any circumstances, disclose their network username or password, to anyone or allow them to access to Health Board data. Where Microsoft Authenticator is used staff must be ensure the device is protected by a PIN number or biometrics.

Staff working remotely by using portable devices or removable media must keep equipment, files and media locked out of sight during transit, and must also ensure any equipment is not left either unattended or insecure when off site to prevent accidental loss and unauthorised access at all times, including within their home. Particular care must be taken when media and equipment are taken on to public transport.

Staff travelling to blocked countries are required to request a block exemption if they are required to access Hywel Dda data.

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 connect any privately owned equipment to the Health Board's network
- Not store data on equipment unless supplied by the Health Board
- Not send person identifiable or confidential data to home (internet) e-mail addresses
- Keep equipment and files locked out of sight during transit
- Ensure equipment/files are adequately packaged in transit to prevent damage or tampering
- Not dispose of any media (including paper) off-site

Training

All staff will be required to have appropriate information governance training which will include guidance on transfer of personal information. A range of training methods will be considered in relation to identified needs and other training and awareness raising around transfer of personal information will be arranged as appropriate.

Implementation

All staff must adhere to this policy and comply with applicable UK legislation.

Failure to follow these policies may lead to disciplinary action being taken against the member of staff and could potentially lead to criminal investigation and potential prosecution.

As part of the information governance monitoring processes, regular audit of information flows will be carried out to ensure personal information is being transferred appropriately.