Enw y Grŵp/Is-Bwyllgor: Name of Group:	**Information Governance Sub-Committee (IGSC)**
Cadeirydd y Grŵp/Is-Bwyllgor: Chair of Group:	**Huw Thomas, Director of Finance**
Cyfnod Adrodd: Reporting Period:	**3 October 2023**

Y Penderfyniadau a'r Materion a Ystyriodd y Grŵp/Is-Bwyllgor:
Key Decisions and Matters Considered by the Group:

Clinical Coding Update
The Information Governance Sub-Committee received an update on the clinical coding position and were assured that the 95% target of records clinically coded within one reporting month post episode discharge end date is continuing the achieved.

The Sub-Committee received the finalised Digital Health and Care Wales Audit Report for 2022/23, and noted the following:

- Achieved above the recommended accuracy for all 4 targets - primary diagnosis, secondary diagnosis, primary procedure, and secondary procedure coding.
- In terms of the 421 episodes examined, 279 (66.27%), contained no errors in any position.

Overall, the Clinical Coding Department at Hywel Dda University Health Board (HDdUHB) achieved above the recommended levels of accuracy of coded data. The recommendations included within the report were noted by the Sub-Committee and will form part of the work programme for the clinical coding team and will be monitored by the Sub-Committee.

HDdUHB's Information Governance Audits
The Sub-Committee noted that The Information Governance Team has now completed audits in Withybush Hospital, Glangwili Hospital and Prince Philip Hospital. The purpose of the audit is to identify any information governance risks, information security risks and patient confidentiality risks to seek assurance that the relevant procedures and protocols in relation to Information Governance are being adhered to and that actions are being taken to protect data and assets held. The initial themes following the audits are as follows:

- Requirement to improve awareness on the importance of following procedural advice for requests such as Subject Access and Police Requests.
- Raising awareness about inappropriate access by staff to medical information.

The Sub-Committee were assured that all of the above have been included Information Governance Workplan.

Information Governance Workplan 2023-2024
The Sub-Committee noted the proposed workplan for the Information Governance Team. The Information Governance work plan highlights a number of the areas that cover off or contribute to the ensuing that the organisation and individuals personal and corporate information, is

compliant in line with current and future legislation. The workplan and any preceding plans will focus on a programme of work for the HDdUHB to include but not limited to:-

- Management of the Information Asset function.
- Assessments (including those that are self-assessed) are completed in a timely manner and reflect current arrangements to provide applicable persons with assurance that HDdUHB handles and controls information in an ethical and lawful manner; and all new or existing identifiable information use and processes are Data Protection Impact Assessed (Privacy by Design) and involve Information Governance input at the earliest possible juncture.

The Sub-Committee thanked the Information Governance Team for the comprehensive workplan and noted that updated will be returned for consideration on a quarterly basis.

Information Commissioner Office (ICO) Notifications
Since April 2023, there have been 4 occurrences when a notification to the Information Commissioner's Office (ICO) has been required. The following table highlights the current notifications:

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Open	0	0	1	1	1	1	-	-	-	-	-	-	4
Closed	-	-	-	-	-	-	-	-	-	-	-	-	0
Total	0	0	1	1	1	1	0	0	0	0	0	0	4

All the above cases are still in progress and are awaiting responses from the ICO.

Information Governance Compliance Update
The Sub-Committee received the update from the Information Governance Team towards the data protection compliance. The Sub-Committee noted the following:

- The continual work of the Team around the completion and review of Information Asset Registers (IARs). The impact on creating IARs for Managed Practices.
- An amendment to the Website Privacy Notice, to ensure compliance with accessibility standards.

Retention and Destruction of Patient Records
The Sub-Committee received and welcomed the update on the Digital Health Records Scanning Programme (DHRP), and the intention to proceed with the destruction of paper and transitional digital data copies in-line with the Health Board's agreed retention periods and destruction schedules for the inactive health records currently in the care of the three scanning providers that were commissioned in January 2022. The Sub-Committee had a long debate on advantages and disadvantages of the recommendations outlined within the paper, and after careful consideration the Chair agreed to work with the DHRP programme, Legal and Information Governance, to bring an update paper to the November 2023 meeting for further deliberation.

Cyber-Security and Network and Information Systems (NIS) Directive Update
A separate report has been prepared for presentation to the In-Committee Sustainable Resources Committee to provide an update on progress of cyber-security.

Policies for approval

- 224 – Information Classification Policy – Pending approval of IGSC Chair's action by the IGSC, the policy will be removed, as it is no longer fit for purpose. A new policy will be issued under the All-Wales Information Governance Policy.
- 281 – Mobile Working Policy – Following a full review process with minimal changes, this policy was approved by IGSC on 24 October 2022 but required an equality impact assessment to be undertaken and signed by the Equalities team. This has now been completed and presented for Sustainable Resources Committee approval (Appendices 1 and 2).
- 301 – User account management policy – Following a full review process minimal changes were noted, this policy was approved by IGSC on 24 October 2022 but required an equality impact assessment to be undertaken and signed by the Equalities team. This has now been completed and presented for Sustainable Resources Committee approval (Appendices 3 and 4).
- 172 – Confidentiality policy – following a full review process minimal changes were noted, and this policy was approved by IGSC on 13 April 2023 but required an equality impact assessment to be undertaken and signed by the Equalities team. This has now been completed and presented for Sustainable Resources Committee approval (Appendices 5 and 6).
- 238 – Information Governance Framework – Following a full review process undertaken by the IG team which they determined had minimal changes, this policy was approved by IGSC on 13 April 2023 but required an equality impact assessment to be undertaken and signed by the Equalities team. This has now been completed and presented for Sustainable Resources Committee approval (Appendices 7 and 8).
- 279 – Third Party Supplier Security Policy – this policy is currently outside the review period however a full review is underway, and as such the extant policy still remains fit for purpose. The revised policy is being reviewed and input is required from Procurement services (Shared Services), and it will be tabled at the next IGSC meeting in November 2023.

Materion y Mae Angen Ystyriaeth neu Gymeradwyaeth Lefel y Pwyllgor Adnoddau Cynaliadwy:
Matters Requiring Sustainable Resources Committee Level Consideration or Approval:

Note the change to the **Hywel Dda Health Board Privacy Notice**

Approve the following four policies:

- 281 Mobile Working Policy
- 301 User Account Management Policy
- 172 Confidentiality Policy
- 238 Information Governance Framework

Approve the removal of policy number 224 Information Classification policy from the internet.

Approve the use of policy number 279 Third Party Supplier Security Policy as fit for purpose pending the All-Wales documentation.

Risgiau Allweddol a Materion Pryder: **Key Risks and Issues / Matters of Concern:**
• The wider strategic issue of the storage of records and boxes within external storage companies.
Busnes Cynlluniedig y Grŵp/Is-Bwyllgor ar Gyfer y Cyfnod Adrodd Nesaf: **Planned Group/Sub-Committee Business for the Next Reporting Period:**
Adrodd yn y Dyfodol: **Future Reporting:**
• Information Asset Owners and Information Asset Mapping Update • Data Quality and Clinical Coding • Information Governance Risk Register • Information Governance Toolkit improvement plan • Update on Cyber Security/Network & Information Systems Regulations (NISR) • Caldicott Register to be returned to the IGSC meetings • Digital/IG Policies and Procedures
Dyddiad y Cyfarfod Nesaf: **Date of Next Meeting:**
30 November 2023

Mobile Working Policy

Policy information

Policy number: 281

Classification:
Corporate

Supersedes:
Previous Versions

Version number:
3.0

Date of Equality Impact Assessment:
02/10/2023

Approval information

Approved by: Sustainable Resources Committee (SRC)
Date of approval:
Enter approval date
Date made active:
Enter date made active (completion by policy team)
Review date:
Enter review date (normally three years from approval 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
422 - Consumer Device Policy (Smartphones / Tablets)

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub Committee
24/10/2022

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1.0 – New Policy
2.0 – Revised
3.0 – Full Review

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 ~~Informaton~~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 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 whether or not 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 memorykey 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.

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, 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 facility to work remotely.

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.

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. They must agree with their manager how they will comply with this policy when working away from Health Board controlled premises.

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.

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.

Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

Equality Impact Assessment (EqIA) Screening Template

The Equality Impact Assessment Screening Template is a short exercise that involves looking at the overall proposal and deciding if it is relevant to the Public Sector Equality Duty, and other key areas.

The questions in the Screening Template below will help you to decide if the proposal is relevant to the Equality Act 2010 and whether a detailed EqIA is required. The key question is whether the proposal is likely to an impact (either positive or negative) on any of the protected characteristics.

Quite often, the answer may not be obvious, and staff, service-user or provider information will need to be considered to make a preliminary judgment.

There is no one size fits all approach, but the screening process is designed to help fully consider the circumstances and to inform evidence-based decisions.

Note: If the proposal is of a significant nature and it is apparent from the outset that a full Equality Impact Assessment (EqIA) will be required, then it is not necessary to complete the Screening Template and you can proceed to complete the full EqIA.

What to do:

In general, the following questions all feed into whether an EqIA is required:

- How many people is the proposal likely to affect?
- How significant is its impact?
- Does it relate to an area where there are known inequalities?

At this initial screening stage, the point is to try to assess obvious negative or positive impacts.

You will need to provide sufficient information within the template to justify the assessment of impact.

If a negative/adverse impact has been identified (actual or potential) during completion of the screening tool, a full EqIA must be undertaken.

If no negative / adverse impacts arise from the proposal, it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded.

On completion of the Screening Template, staff should:

- Check that all sections of the template are fully completed.
- Ensure that the Project/Policy owner has signed off the Screening Template.
- Send a copy of the completed template along with the related policy to the Diversity & Inclusion Team for them to review – email this to Inclusion.hdd@wales.nhs.uk

Date of commencement of Screening Assessment:	**22 Sep 23**
Screening conducted by (name and email address):	**Gavin Jones Gavin.jones2@wales.nhs.uk**
Title of programme, policy or project being screened:	**Mobile Working Policy**

Description of the programme/policy/project being screened (including key aims and objectives)

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 aim of this document is:

- 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.

Evidence considered (including staff and population data, relevant research, expert and community knowledge etc.)

Only the contents of the policy have been considered against the requirements within this template.

Assess which protected characteristics will potentially be affected by the proposal:

Group	Positive Impact	Negative Impact	No Impact
Age Is it likely to affect older and younger people in different ways or affect one age group and not another?			Yes
Disability Those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes			Yes
Gender Reassignment Consider the potential impact on individuals who either: • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth			Yes
Marriage / Civil Partnership This also covers those who are not married or in a civil partnership.			Yes
Pregnancy and Maternity Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave			Yes
Race / Ethnicity People of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, gypsies/travellers, asylum seekers and migrant workers.			Yes
Religion or Belief The term 'religion' includes a religious or philosophical belief.			Yes
Sex Consider whether those affected are mostly male or female and where it applies to both equally does it affect one differently to the other?			Yes
Sexual Orientation			Yes

Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes.			

Consider the potential impacts of the programme/policy/project on the following wider determinants:

Additional Determinants	Positive Impact	Negative Impact	No Impact
Armed Forces Community Consider members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.' For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see: **Armed-Forces-Covenant-duty-statutory-guidance**			Yes
Socio Economic Duty Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered. For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resource please see: more-equal-wales-socio-economic-duty			Yes
Welsh Language Please note opportunities for persons to use the Welsh language and treating the Welsh language no less favourably than the English language.			Yes

Summary of Potential Impacts Identified

Positive Impacts

N/A

Negative Impacts

N/A

Has the screening identified any negative impacts? **If yes, a full Equality Impact Assessment will need to be undertaken.**	~~Yes~~	No

If No negative impacts were identified, please give full justification here

The policy is applicable to all Health Board staff and does not have any specific positive or negative impact on the groups listed above. All staff must comply with the policy.

Screening Completed by:	Name	Gavin Jones
	Title	Head of Digital Operations
	Contact details	Gavin.jones2@wales.nhs.uk
	Date	2 Oct 23
Screening Authorised by: (Project / Policy Owner)	Name	Anthony Tracy
	Title	Digital Director
	Contact details	Anthony.Tracey@wales.nhs.uk
	Date	2 Oct 23
Seen by Diversity & Inclusion Team:	Name	Alan Winter
	Title	Senior Diversity & Inclusion Officer
	Contact details	Alan.winter@wales.nhs.uk
	Date	2/10/2023

User Account Management Policy

Policy information

Policy number: 301

Classification:
Corporate

Supersedes:
N/A

Version number:
4.0

Date of Equality Impact Assessment:
02/10/2023

Approval information

Approved by:
Sustainable Resources Committee

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:
This policy states the policy for user account management within Hywel Dda University Health Board.

Scope:
This policy applies to all users of information systems that reside within Hywel Dda or are part of a national service which hosts a Hywel Dda database. The users could be full-time employees as well as staff from elsewhere in NHS Wales or third-party contract staff and locums.

To be read in conjunction with:
837 - All Wales Information Security Policy (opens in new tab)
494 – All Wales Email Policy (opens in a new tab)

Patient information:
Include links to Patient Information Library

Owning group: IGSC
24/10/2022

Executive Director job title:
Huw Thomas - Director of Finance

Reviews and updates:
1.0 - New Policy - September 2012
2.0 - Review - 23.02.2016
3.0 - DPA Reference changes - 26.06.2018
4.0 - Review following NIS-R assessment

Keywords:
User Account, Computer Account, Network Account, Citrix Account, User Access, Computer Access, Network Access, Citrix Access, New Password, Change Password, Locum.

Glossary of Terms:
Nadex - National Active directory and exchange service
ESR - Electronic Ssstaff Rrecord
OD - Organisation Development
NHS - National Health Service
A&E - Accident and Emergency

Contents

Introduction
This document defines the user access management policy for Hywel Dda University Health Board ensuring account access is authorised and underpins the requirements of the Data Protection Act 2018/General Protection Regulations 2016 or any subsequent legislation to the same effect and other relevant legislation.

Policy statement
This document defines the user access management policy for Hywel Dda University Health Board and this policy applies to all health board information systems and services hosted both internally and externally, included nationally hosted systems.

The policy describes the registration and de-registration process of user accounts and applies to new starters, leavers and those moving roles within the health board as well as temporary locum staff. Access to Health Board information systems will be subject to approval by the relevant Information Asset Owners / Information Asset Administrators.

Scope
This policy applies to all users of information systems that reside within Hywel Dda or are part of a national service which hosts a Hywel Dda database.

The users could be full-time employees as well as staff from elsewhere in NHS Wales or third party contract staff and locums.

Aim
The aim of this document is to:
- Ensure the Health Board can have assurance that user accounts used to access clinical and administrative systems are managed appropriately and ensure the confidentiality of Health Board data.

Objectives
The aim of this document will be achieved by the following objectives:
- Ensuring that appropriate procedures are in place to manage the process for new user accounts, amendments to user privileges and those staff which have left the organisation.

Procedures
The Digital Services department will follow the relevant procedure to ensure starters, leavers and role changes are undertaken in line with requirements of the national Active Directory (Cymru).

New users
Access to Hywel Board information systems is controlled through a formal user registration process beginning with a formal request from Workforce & OD or from a line manager using the automated user provisioning service.

Each user is identified by a unique user ID which is part of the NHS Wales Cymru directory and will conform to national naming standards. Where possible this ID will be used on systems that do not use Cymru to authenticate users to enable audit and faster de-provisioning of users.

New users will have a standard level of access which will include the following:-

- PC login
- Microsoft One Drive for storing personal documents
- Office 365 (Email and Web versions of Office)
- Microsoft Teams
- Intranet
- Internet

Additional access levels if required in their role can be authorised by their line manager during the request process.

The use of generic usernames is only suitable for open access PC's and where the application containing Health Board data is protected by an individual username and password, and where possible their use will be minimised. Acceptable areas include:-

- Ward PC's which stay logged in at all times.
- Unscheduled care departments where fast access is required (A&E, Critical Care).

Generic accounts can also be used for shared mailboxes, but it will not be possible to login using these accounts and access will only be granted through a user's mailbox.

To request access then the relevant electronic form needs to be completed which is available on the Digital Services portal.

Each user will be required to electronically confirm the form to ensure a record of their access rights and that they understand the conditions of access and abide by the Health Board's policy and procedures.

Passwords will be issued automatically to the line manager. The user will be required to ensure their details are up to date and create related security question which will be used by the Digital Service Desk to ensure positive identification.

A separate procedure will be in place to ensure short-term accounts (i.e. Locums and Students) are managed appropriately.

Digital Services will maintain a record of all requests on our Service Management tool.

Change of User Requirements

Changed requirements will normally relate to an alteration to the applications used, this must be requested by the line manager using the relevant electronic form which is available in the Digital Services portal. If a user moves to a different role requiring different access levels, the "outgoing" line manager must initiate a change form in order to remove current access levels. The line manager for the new role will also need to initiate a change form to request new levels of access.

Digital Services will maintain a record of all requests on our Service Management tool.

Staff moves between NHS Wales Organisations

When a user moves between NHS Wales organisations the user will have all permissions removed and the user transfer portal will transfer the users email address from Hywel Dda to the receiving organisation.

Any data will be retained in Hywel Dda unless specific agreement is sought from the Senior Information Risk Owner or the Head of Information Governance.

Change of password

Where a user has forgotten their password the Service Desk is authorised to issue a replacement providing he/she already has access to the relevant information system. Where access isn't available the Service Desk will pass the request over to the relevant Information Asset Owner or Information Asset Administrator.

Upon receipt of such a request the Service Desk will:-

- Ensure the request is logged.
- Confirm the identity of the user by confirming their username and their security question
- Issue a temporary, single use, password which will require the user to change at first login.

All passwords will be required to be 11 characters in length and all users are encouraged to setup for Microsoft Multi-Factor Authentication and Self-Service Password Reset. In line with the National Cyber Security Centre the Health Board no longer forces password changes or the use of complex requirements.

Removal of Users

As soon as an individual leaves the Health Board's employment, all his/her login account must be disabled and accounts will be retained for 12 months before being deleted Users at Band 6 and higher will have litigation hold applied on Office 365 so electronic mail will be retained after the account has been removed to meet the requirements of the COVID pandemic public enquiry.

As part of the employee termination process the Digital Service Desk will have electronic notification from ESR. Once received Digital will disable the account in line with the termination date and follow the procedure for dealing with leavers, the Digital Service Desk will inform system administrators of leavers when their systems are affected and a report of leavers on a monthly basis will be provided to the Information Asset Owners Group. This process will be automated in line with planned improvements to the starters, leavers and movers process.

It is the line manager's responsibility to ensure any Digital equipment assigned to the user is returned to the Digital department including laptops, phones, Security tokens and encrypted USB memory keys.

Leaver's files and emails will be managed as per the 494 – All Wales Email Use Policy – opens in a new tab.

Records of leavers will be stored against the relevant Service Management records.

Digital Services will also run monthly reports of stale accounts identifying those accounts which haven't been used for 3 months. Any identified will be automatically disabled, have their Microsoft licences removed and moved to a holding area. These disabled accounts will be deleted after a further 12 months. Digital will cross check with ESR those staff on long-term sick and maternity / paternity leave before actioning at 3 and 12 months.

Privileged Accounts

"Special privileges" are those allowed to the Digital department or Information Asset Administrators allowing access to data and information.

Privileged access must be authorised by the Deputy Digital Director or the relevant Information Asset Owner and records kept of who has this access. The list of privileged accesses will be checked and confirmed by the Cyber Security Manager / NADEX Service Management Board representative on a three monthly basis.

Review of User Access Rights

The NADEX Service Management Board representative will institute a review of all access rights to the network once a quarter which is designed to positively confirm all users.

Annually the Cyber Security Manager will institute a review of access to applications. This will be done in co-operation with the application owner and will be designed to positively re-confirm all users; all other logons will be deleted. In exceptional circumstances (e.g. Maternity Leave) accounts which have not been used for some time will not be deleted, but will continue to be monitored.

The review will be conducted as follows:-

- The Information Asset Owners / Information Asset Administrators for each system will generate a list of users (apart from systems which use Cymru as an authentication source)
- The list will be sent to the Cyber Security Manager who will confirm that all users are authorised to still use the system through automated methods where possible
- The Cyber Security Manager will maintain records off:-
  - Audits completed
  - System administrator responses
  - Records of actions taken

Responsibilities

Users:

- All users of Hywel Dda systems must be made aware of the contents and implications of the user access management policy and the general requirement to ensure that information systems must be kept secure.
- Irresponsible or improper actions by users may result in disciplinary actions(s).
- Keep their user details up-to-date and accurate using self-service tools available on the Intranet.
- Sign up for Microsoft Multi-Factor authentication
- Sign up for the Microsoft Self-Service Password Reset tool
- Report to the Digital Service Desk if a user feels they have inappropriate permissions or access.
- Ensure any requests for new user accounts or modification to permissions are completed using the relevant electronic forms on the Digital Services Portal.

- Keep their passwords secure and confidential and do not share.
- If a user changes their role within the Health Board, it is their responsibility to ensure that they do not continue to use access privileges from a previous role and to notify their manager that their access rights should be changed.

Deputy Digital Director
- Ensure the production of all relevant operating procedures reflecting the requirements of this policy.
- Ensure these procedures are followed by all Digital staff.
- Ensure Service Desk is aware of their responsibilities in line with this policy.
- Ensure effective management of privileged accounts.
- Promote the Cymru domain as an authentication source.

Service Desk
- Follow the associated procedures created to implement this policy.
- Ensure Service Management records are accurate and kept up-to-date.

Cyber Security Manager's Responsibilities
- Undertake review of access rights to the network and Hywel Dda applications and act on the results of these audits.
- Ensure records are accurate and kept up-to-date.
- Encouraging, monitoring and checking compliance with this policy.
- Promoting awareness and providing guidance on this policy.

Information Asset Owners / Information Asset Administrators
- Work with the Cyber Security Manager in undertaking user access reviews.
- Ensure records are accurate and kept up-to-date.

Workforce and Organisational Development
- Ensuring ESR notifications are received by the Digital Service Desk of those staff which have left the organisation.

Line Manager's Responsibility
- Ensuring all employees are made aware of their security responsibilities as indicated in this policy.
- Ensure that all users under their management are given the appropriate access rights for their role.
- Notify Digital Services when users leave the Health Board or change their role within the Health Board, e.g. by moving to a different department or function.

Training

Training relating to this policy must take place during the induction programme for new staff or as part of refresher training at least every two years as part of the Information Governance and Information Security training.

Implementation

This policy will be implemented through procedures undertaken by the Digital Service Desk and Information Asset Owners Group.

Further Information

Some of the guidelines in this policy are laid down by the National Active Directory & Exchange Service Management Board.

Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

Equality Impact Assessment (EqIA) Screening Template

The Equality Impact Assessment Screening Template is a short exercise that involves looking at the overall proposal and deciding if it is relevant to the Public Sector Equality Duty, and other key areas.

The questions in the Screening Template below will help you to decide if the proposal is relevant to the Equality Act 2010 and whether a detailed EqIA is required. The key question is whether the proposal is likely to an impact (either positive or negative) on any of the protected characteristics.

Quite often, the answer may not be obvious, and staff, service-user or provider information will need to be considered to make a preliminary judgment.

There is no one size fits all approach, but the screening process is designed to help fully consider the circumstances and to inform evidence-based decisions.

Note: If the proposal is of a significant nature and it is apparent from the outset that a full Equality Impact Assessment (EqIA) will be required, then it is not necessary to complete the Screening Template and you can proceed to complete the full EqIA.

What to do:

In general, the following questions all feed into whether an EqIA is required:

- How many people is the proposal likely to affect?
- How significant is its impact?
- Does it relate to an area where there are known inequalities?

At this initial screening stage, the point is to try to assess obvious negative or positive impacts.

You will need to provide sufficient information within the template to justify the assessment of impact.

If a negative/adverse impact has been identified (actual or potential) during completion of the screening tool, a full EqIA must be undertaken.

If no negative / adverse impacts arise from the proposal, it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded.

On completion of the Screening Template, staff should:

- Check that all sections of the template are fully completed.
- Ensure that the Project/Policy owner has signed off the Screening Template.
- Send a copy of the completed template along with the related policy to the Diversity & Inclusion Team for them to review – email this to Inclusion.hdd@wales.nhs.uk

Date of commencement of Screening Assessment:	**22 Sep 23**
Screening conducted by (name and email address):	**Gavin Jones** **Gavin.jones2@wales.nhs.uk**
Title of programme, policy or project being screened:	**User Account Management Policy**

Description of the programme/policy/project being screened (including key aims and objectives)

This policy states the policy for user account management within Hywel Dda University Health Board.

The aim of this document is to:

- Ensure the Health Board can have assurance that user accounts used to access clinical and administrative systems are managed appropriately and ensure the confidentiality of Health Board data.

Evidence considered (including staff and population data, relevant research, expert and community knowledge etc.)

Only the contents of the policy have been considered against the requirements within this template.

Assess which protected characteristics will potentially be affected by the proposal:

Group	Positive Impact	Negative Impact	No Impact
Age Is it likely to affect older and younger people in different ways or affect one age group and not another?			Yes

Disability Those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes			Yes
Gender Reassignment Consider the potential impact on individuals who either: • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth			Yes
Marriage / Civil Partnership This also covers those who are not married or in a civil partnership.			Yes
Pregnancy and Maternity Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave			Yes
Race / Ethnicity People of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, gypsies/travellers, asylum seekers and migrant workers.			Yes
Religion or Belief The term 'religion' includes a religious or philosophical belief.			Yes
Sex Consider whether those affected are mostly male or female and where it applies to both equally does it affect one differently to the other?			Yes
Sexual Orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes.			Yes

Consider the potential impacts of the programme/policy/project on the following wider determinants:

Additional Determinants	Positive Impact	Negative Impact	No Impact
Armed Forces Community Consider members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.' For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see: **Armed-Forces-Covenant-duty-statutory-guidance**			Yes
Socio Economic Duty Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered. For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resource please see: more-equal-wales-socio-economic-duty			Yes
Welsh Language Please note opportunities for persons to use the Welsh language and treating the Welsh language no less favourably than the English language.			Yes

Summary of Potential Impacts Identified

Positive Impacts

N/A

Negative Impacts

N/A

Has the screening identified any negative impacts? **If yes, a full Equality Impact Assessment will need to be undertaken.**	~~Yes~~	No

If No negative impacts were identified, please give full justification here

The policy is applicable to all Health Board staff and does not have any specific positive or negative impact on the groups listed above. All staff must comply with the policy.

Screening Completed by:	Name	Gavin Jones
	Title	Head of Digital Operations
	Contact details	Gavin.jones2@wales.nhs.uk
	Date	2 Oct 23
Screening Authorised by: (Project / Policy Owner)	Name	Anthony Tracy
	Title	Digital Director
	Contact details	Anthony.Tracey@wales.nhs.uk
	Date	2 Oct 23
Seen by Diversity & Inclusion Team:	Name	Alan Winter
	Title	Senior Diversity & Inclusion Officer
	Contact details	Alan.winter@wales.nhs.uk
	Date	2/10/2023

Confidentiality Policy

Policy information

Policy number: 172

Classification:
Corporate

Supersedes:
Previous versions

Version number:
7

Date of Equality Impact Assessment:
20.06.2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:

Date made active:

Review date:
Enter review date (normally three years from approval date)

Summary of document:
This policy states our commitment to maintain the confidentiality, Privacy and security of all Classified information and outlines mechanisms for ensuring this takes place.

Scope:
This Policy deals with any information (held in any medium) collected or processed by Health Board staff that is subject to a classified status, as defined in the Health Board's Information Classification policy, that staff work with or come into contact with, however transitory, in the course of their work. Staff includes employees, temporary or agency staff, volunteers, locums and third party contractors.
To be read in conjunction with:
183- Information Security policy (opens in new tab)
201- Disciplinary policy (opens in new tab)
173- Freedom of Information Policy (opens in new tab)

All Records Management policies and Procedures

Owning group:
Information Governance Sub-committee (IGSC)*13/04/2023*

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1 – New Policy – 01.03.2011
2 – Amended – 28.04.02023
3 – Revised – 26.06.2018
4- Revised –

Keywords
Confidential, Confidentiality

Glossary of terms

Contents

Introduction

Service users of health and social care are entitled to expect that the information they entrust to their providers of care will be held in the strictest confidence. This requirement has been a cornerstone of the trust that needs to exist between medical practitioner and patient. The trust which allows a patient to divulge intimate details secure in the knowledge that what they say will not be inappropriately divulged. It is not just information security that is important, patients also expect that the professionals involved in their care, will share that information appropriately, reliably, and effectively.

Policy Statement

The Hywel Dda Hywel Dda Health Board (HDdUHB) is committed to protecting the security and privacy of information, regardless of media type, in accordance with applicable laws and regulations. Information is a critical and valuable asset for the HDdUHB. Information security is the protection of information from a wide range of threats in order to ensure business continuity and minimise business risk. The objective of information security is to reduce the risk to the HDdUHB by protecting information, information systems and communications that deliver the information, from failures
of integrity, confidentiality, and availability, whether information is in storage, processing, or transmission. Information security is seen as an enabler to achieve HDdUHB business strategy and objectives and to avoid or reduce relevant risks.

This policy is intended to establish an organisational framework for the HDdUHB's policies related to information Governance and its security.

Scope

This Policy deals with any information (held in any medium) collected or processed by Health Board staff that is subject to a classified status, as defined in the Health Board's Information Classification policy that staff work with or come into contact with, however transitory, in the course of their work. Staff includes employees, temporary or agency staff, volunteers, locums and third party contractors.

Aims

There are a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. The aim of this policy is to assist staff in carrying out their duties lawfully by identifying these statutory requirements and providing best practice guidance.

Objectives

This policy assists staff in understanding the interrelationship between the ethical considerations, professional principles and laws in relation to the using or sharing of confidential information and by assisting staff in addressing and understanding their duty under common law to maintain confidentiality and where that duty may be overridden. However, this document should not be seen as a substitute for professional legal advice.

Policy

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within HDdUHB and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All staff working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 2018, UK General Data Protection Regulation 2016, or any subsequent legislation to the same effect. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

It is important that the Health Board protects and safeguards person-identifiable and confidential business information that it gathers, creates, processes, and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current Welsh NHS Encryption Guidance, or a business case has been approved by Digital Services.

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes the Health Board's confidential business information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

How to report a breach of this policy and what should be reported can be found in Appendix C.

The legal definition of confidential information can be found in Appendix D.

Roles and Responsibilities

The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that HDdUHB policies comply with all legal, statutory, and good practice guidance requirements.

The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

The Information Governance Sub-Committee

The Information Governance Sub-Committee oversees the development and implementation of Information Governance in the Health Board and ensure that the organisation complies with supporting the Legal and NHS Mandatory Framework with regard to Information Governance.

Director with responsibility for Workforce and Organisational Development (W&OD)

The Director with responsibility for W&OD is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate induction for all staff.

Senior Managers

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure identified in the IT Security policy.

Head of Information Governance

The Head of Information Governance is responsible for maintaining the accuracy of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

All ~~staff~~Staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Duty of Confidentiality at Common Law. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported.

Corporate Level Procedures

Principles

All staff must ensure that the following principles are adhered to: -

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person--identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure must be discussed with either your Line Manager or the Corporate Services Information Governance Team.

HDdUHB is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Access to rooms and offices where terminals are present, or person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks of confidential or sensitive material at the end of each day. In particular, they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts, and fax messages must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

Disclosing Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and ensure that only the minimal amount necessary is disclosed.

When information can be disclosed:

- When it is effectively anonymised.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian when appropriate.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

If staff have any concerns about disclosing information, they must discuss this with their Line Manager, or the Information Governance staff. Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements whether under the Wales Accord on the Sharing of Personal Information) WASPI, Memorandum of Understanding (MOU's) or other regimes please contact the Information Governance team.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Safe Haven Procedure for guidance on the safe transfer of confidential or person-identifiable information.

Transferring patient information by email to anyone outside Welsh Health network may only be undertaken by using encryption as per the current HDdUHB All Wales Information Security Policy. Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry HDdUHB information with them which could be confidential in nature e.g., on a laptop, USB stick or paper documents. Taking home/-removing paper documents that contain person-identifiable or confidential information from HDdUHB premises is discouraged. When working away from HDdUHB locations staff must ensure that their working practice complies with HDdUHB policies and procedures.

To ensure the safety of confidential information, staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations. As a general rule, staff must minimise the amount of person-identifiable information that is taken away from HDdUHB premises. If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e., windowless envelope, suitable bag, etc. prior to being taken out of HDdUHB buildings.
- Confidential information is kept out of sight whilst being transported.

If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person identifiable or confidential information on a privately--owned computer or device (including mobile devices).

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes, and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed.

Steps must be taken to ensure physical safety and security of person identifiable, or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gGross -misconduct which may result in summary dismissal.

Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate Health

Board purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act/UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the HDdUHB.

If staff have concerns about this issue, they should discuss it with their Line Manager or Information Governance Team.

Confidentiality Audits
Good practice requires that all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by Digital Services in conjunction with Information Governance team through a programme of audits.

Distribution and Implementation
This document will be made available to all Staff via the HDdUHB intranet site, and a global notice will be sent to staff notifying them of the release of this document.

A link to this document will be provided from the Publication scheme on the HDdUHB intranet site.

Training
Links to the Health Boards policy pages will be provided at staff induction and during local staff training sessions.

Monitoring
Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance team, together with independent reviews by both Internal and External Audit on a periodic basis. The Head of Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

Equality Impact Assessment
This document forms part of the Health Board's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities. As part of its development this document and its impact on equality has been analysed and no detriment identified.

Who to contact:

Should you have any queries in relation to this policy please email the Information Governance Team at Information.Governance3@wales.nhs.uk, alternatively, you can contact:

Data Protection Officer (DPO) at: DPO.HDD@wales.nhs.uk,

Senior Information Risk Officer (SIRO) at: SIRO.HDD@wales.nhs.uk

Caldicott Guardian at: caldicottguardian.hdd@wales.nhs.uk

Appendix A - Do's and Don'ts

Dos

1. Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working in or on behalf of the Health Board.
2. Do clear your desk at the end of each day if possible, keeping all portable records that contain person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
3. Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any period of time.
4. Do ensure that you cannot be overheard when discussing confidential matters.
5. Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
6. Do share only the minimum information necessary.
7. Do transfer person-identifiable or confidential information securely when necessary, i.e., use encryption to send confidential information to a non NHS email account or use a secure government domain e.g. gsi.gov.uk if possible.
8. Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
9, Do report any actual or suspected breaches of confidentiality.
10. Do participate in induction, training and awareness sessions on confidentiality issues.

Don'ts

11. Don't share passwords or leave them lying around for others to see.
12. Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
13. Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
14. Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and NHS Frameworks

The Health Board is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and agents of HDdUHB, who may be held personally accountable for any breaches of information security for which they may be held responsible.

The Health Board shall comply with the following legislation and guidance as appropriate:

The Data Protection Act/ UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect regulates the use of "personal data" and sets out seven principles to ensure that personal data is:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The UK General Data Protection Regulation contains clauses relating to the rights of data subjects namely: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making.

The Caldicott Report (1997) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared, a further review took place in January 2012 which resulted in a seventh principle being added. In December 2020 an 8th principle was also added:

1. Justify the purpose for using patient-identifiable information.

2. Don't use patient identifiable information unless it is absolutely necessary.

3. Use the minimum necessary patient-identifiable information.

4. Access to patient-identifiable information should be on a strict need to know basis

5. Everyone should be aware of their responsibilities

6. Understand and comply with the law.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

8. Inform patients and service users about how their confidential information is used.

The Human Rights Act (1998)

Article 8 of which refers to an individual's "*right to respect for their private and family life, for their home and for their correspondence"*. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) this Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

Each offence includes the making, supplying or obtaining articles for use in perpetrating these offence.

The Code of Confidentiality for Health and Social Care in Wales (2005) outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or We have special permission because the public good is thought to be of greater importance than your confidentiality, and if we share information without your permission, we will make sure that we keep to the Data Protection Act, the Code of Confidentiality for Health and Social Care in Wales and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the Health Board understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix C: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. All breaches should be reported either on Datix or via email. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Information Governance staff. The following list gives examples of

breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to Health Board systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act or duty of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information in any media.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person identifiable information in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or the Information Governance Manager should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Information Governance Sub Committee and the information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Legal definition of Confidentiality

Common law jurisdictions have established torts (breaches of duties not under contract with liability for damages) to protect individuals' rights to privacy. A number of common law torts afford protection to individuals' private interests and their confidential information. With regard to the use and disclosure of personal information, or information provided by third party organisations, the tort of breach of confidence is clearly the most relevant. Where the information is created internally and for internal use, the Common law Duty of Confidentiality clearly cannot apply, and then the Common Law Duty of Fidelity becomes the most relevant medium for action.

For something to be confidential, three elements are normally required if, apart from as a result of a contract, a case of breach of confidence is to succeed[1]".

First, the information itself, must "**have the necessary quality of confidence about it**". The information must be of a confidential nature, it cannot be trivial in content[2] "…something which is public property and public knowledge" cannot *per se* provide any foundation for proceedings for breach of confidence. However confidential the circumstances of communication there can be no breach of confidence in revealing to others something which is already common knowledge.

Secondly, that information must have been imparted in circumstances importing an obligation of confidence. The second requirement is that the information must have been communicated in circumstances importing an obligation of confidence, e.g. the doctor patient relationship, many professional relationships have this obligation. However secret and confidential the information there can be no binding obligation of confidence though, if that information is blurted out in public or is communicated in other circumstances which negative any duty of holding it confidential.

Thirdly, there must be an unauthorised use of that information to the detriment of the confider.

Confidence is not absolute and may be breached where:

- If a person has provided consent for the disclosure of their information.
- If there is a legal requirement to disclose information.
- If it is in the public interest to disclose information.

The basis of the public interest test may be summed up as follows "…although the basis of the law's protection of confidence is that there is a public interest that confidences should be

[1] Coco v A.N.Clarke (Engineers Ltd [1969] RPC 41

[2] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948) 65 R.P.C. 203;

preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure"[3]

A duty of confidence can also be enshrined in the contracts, to which all employees, are subject. The obligation of confidence may arise by virtue of a contract that imposes duties of confidence, or by the circumstances. In employment contracts, employees are under a fiduciary duty, known as fidelity, to their employers, which imports (or implies) an obligation on their part to refrain from disclosing employers' business to third parties without consent. Similarly, third parties and contractors are equally under a duty as a result of clauses in contracts.

Nothing in this policy will impinge on any rights enshrined in the Public Interest Disclosures Act (1998) or article 10 of the Human Rights Act (1998).

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the UK General Data Protection (2016) or the Data Protection Act (2018) refers to personal information about:

• Race or ethnic origin

• Political opinions

• Religious or similar beliefs

• Trade union membership

• Physical or mental health or condition

• Sexual life

• Commission or alleged commission of any offence, or

• Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

[3] Attorney General v Guardian Newspapers (No 2)[1990] 1 AC 109

APPENDIX E: GILLICK COMPETANCE / FRASER GUIDELINES

It is a principle of the law in England and Wales, that consent is needed before medical treatment is commenced on a patient. Without the consent of the patient a criminal offence is committed and the patient may bring a civil action against the health-care professional who initiated the treatment. The fact that a patient may be a child, who is under the age of 18 years in English law, does not remove the need for consent to be provided. The Family Law Reform Act [1969] section 8(1) states “The consent of a minor who has attained the age of sixteen years to any surgical, medical or dental treatment which, in the absence of consent, would constitute a trespass to his person, shall be as effective as it would be if he were of full age; and where a minor has by virtue of this section given an effective consent to any treatment it shall not be necessary to obtain any consent for it from his parent or guardian”. However, this provision did not apply to those under 16 years of age.

In 1982 Mrs Victoria Gillick took her local health authority (West Norfolk and Wisbech Area Health Authority) and the Department of Health and Social Security to court in an attempt to stop doctors from giving contraceptive advice or treatment to under 16- year-olds without parental consent. Mrs Gillick had challenged the lawfulness of Department of Health guidance that doctors could provide contraceptive advice and treatment to girls under the age of 16 without parental consent or knowledge in some circumstances. Mrs Gillick lost the case finally in 1985 when the Law Lords upheld the decision in **Gillick v West Norfolk & Wisbech Area Health Authority [1985] UKHL 7 (17 October 1985)**

When trying to decide whether a child is mature enough to make decisions, people often talk about whether a child is 'Gillick competent' or whether they meet the 'Fraser guidelines'. These labels are often used interchangeably but actually relate to separate though related terms,

Gillick competent, according to Mr Justice Woolf (1982); "...*whether or not a child is capable of giving the necessary consent will depend on the child’s maturity and understanding and the nature of the consent required. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the treatment proposed, so the consent, if given, can be properly and fairly described as true consent."*

Therefore the test is that the young person;

- understands the problem and implications
- understands the risks & benefits of treatment
- understands the consequences if not treated
- understands the alternative options
- understands the implications on the family

- is able to retain (remember) the information
- is able to weigh the pros and cons

- is able to make and communicate a reasoned and weighed decision regarding their wishes.

Fraser guidelines are more specific and originally related only to the provision of contraceptive advice, as Lord Fraser (1985) put it; "...*a doctor could proceed to give advice and treatment provided he is satisfied in the following criteria:*

1) that the girl (although under the age of 16 years of age) will understand his advice;

2) that he cannot persuade her to inform her parents or to allow him to inform the parents that she is seeking contraceptive advice;

3) that she is very likely to continue having sexual intercourse with or without contraceptive treatment;

4) that unless she receives contraceptive advice or treatment her physical or mental health or both are likely to suffer;

5) that her best interests require him to give her contraceptive advice, treatment or both without the parental consent." While Fraser was specifically about contraceptive advice and treatment, the case *Axon, R (on the application of) v Secretary of State for Health [2006] EWHC 37 (Admin)* makes clear that the principles apply to decisions about treatment and care for sexually transmitted infections and abortion, too.

The question of whether the provision of such advice to a person below the age of consent would engage the criminal law was answered by “The Sexual Offences Act 2003”. This Act stated that “, a person is not guilty of aiding, abetting or counselling a sexual offence against a child where they are acting for the purpose of:

- protecting a child from pregnancy or sexually transmitted infection,
- protecting the physical safety of a child,
- promoting a child’s emotional well-being by the giving of advice.

This provision therefore permits health professionals and others working with young people to provide confidential advice or treatment on contraception, sexual and reproductive health to young people under 16.

As a general rule applying the tests provided by the Judge in “Gillick” will be sufficient for your decision to be ‘reasonable in all the circumstances of the case’.

SUMMARY EQUALITY IMPACT ASSESSMENT – CONFIDENTIALITY POLICY – June 2023

Organisation:	Hywel Dda Health Board

Proposal Sponsored by:	**Name:**	**Sarah Bevan**
	Title:	**Information Governance Manager**
	Department:	**Corporate Services**

Policy Title:	Confidentiality Policy

Brief Aims and Objectives of Policy:	The policy outlines the mechanism for ensuring confidentiality, privacy and security of all classified information within the Health Board. The objectives of the policy are:- • To ensure that all staff are aware of and understand the standards that the Health Board expects and requires in relation to confidentiality of both personal and corporate information and to clarify the Board's position with regard to this environment. • To define responsibilities relating to information confidentiality • To clarify applicable legal requirements • To ensure consistent working practices throughout the Health Board.

Was the decision reached to proceed to full Equality Impact Assessment?:		**No ⊙**
	Record Reasons for Decision: The Policy is designed to have an overall positive effect within the organisation in clarifying staffs' roles and responsibilities for maintaining confidentiality within the organisation.	
If no, are there any issues to be addressed?		**No ⊙**
	Record Details:	

Is the Policy Lawful?	**Yes ⊙**	

Will the Policy be adopted?	**Yes ⊙**	
	If no, please record the reason and any further action required:	

Are monitoring arrangements in place?	**Yes** ◉	
	The monitoring of the effectiveness, awareness, compliance and impact of this policy will be the responsibility of the Information Governance Group.	

Who is the Lead Officer?	**Name:**	Sarah Bevan
	Title:	Information Governance Manager
	Department:	Corporate Services
Review Date of Policy:	March 2023	

Signature of all parties:	**Name**	**Title**	**Signature**
	Sarah Bevan	Information Governance Manager	Reviewed on 20.06.2023
	Eiddan Harries	Senior Diversity & Inclusion Officer	20.06.2023

Please Note: An Action Plan should be attached to this Outcome Report prior to signature			

NARRATIVE

Is the purpose of the policy clearly set out – as above

Have those affected by the policy been involved - The Policy has been discussed by the HR Policy Review Group, all members of the Information Governance Sub-Committee, the Integrated Governance Group and Partnership Forum.

Have potential positive and negative impacts been identified – No negative impacts were identified. The Policy will uphold Article 10 of the Human Rights Act.

Monitoring – The monitoring of the effectiveness, awareness, compliance and impact of this policy will be the responsibility of the Information Governance Group.

EqIA HR Policy Review Sub Group 25/1/11
Reviewed July 2014 – No changes needed

Information Governance Framework

Policy information

Policy number: 238

Classification:
Corporate

Supersedes:
Previous versions

Version number:
7

Date of Equality Impact Assessment:
25/04/2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
The Information Governance Framework sets out the standards to be applied across the Health Board for managing information governance including the organisational arrangements, roles, responsibilities and policies.

Scope:
This framework applies to all Health Board staff and the following groups of people who work for or on behalf of the Health Board: committee chairs and members and remunerated expert advisors, agency workers, locums and contractors, secondees, students, volunteers and placement staff

To be read in conjunction with:
172- Confidentiality Policy – (opens in a new tab)
225- Data Protection Policy – (opens in a new tab)
275- Secure Transfer of Personal Information Policy – (opens in a new tab)
279- Third Party Supplier Security Policy– (opens in a new tab)
282- Network Security Policy – (opens in a new tab)
836- All Wales Information Governance Policy – (opens in a new tab)
837- Information Security Policy – (opens in a new tab)

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub-committee (IGSC)*13/04/2023*

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1 – new policy
2 – minor review Feb 2012
3 – framework review 23.4.2013
4 – framework review – 23.09.2014
5 – framework review – 23.02.2016
6 – full review 26.6.2018
7 – full review 27.3.2023

Keywords
Information governance, data protection, SIRO, risk,

Glossary of terms

Term	Definition
Caldicott Principles	A set of principles that lay out how patient information should be handled by NHS organisations to ensure confidentiality is upheld.
Cyber Security	Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.
Data Protection Act	The law around how personal information should be managed by all organisations that use, store and process personal information.
Freedom Of Information Act 2000	A law that gives certain rights to individuals to request access to information held, stored and processed by certain public organisations including Health Boards.
Information Asset	A body of information managed as a single unit so it can be understood, shared, protected and used effectively.
Information Asset Owner	Every information asset must be assigned an owner within the Health Board who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority and experience to understand the contents and

	approve the processing of the record.
Personal Information	Is information that relates to an individual who can be identified from that information or in conjunction with any other information coming into possession of the user of the information. Personal information includes name, address, date of birth or any other unique identifiers such as NHS Number, Hospital Number, National Insurance Number, social care ID etc. It also includes information which, when presented in combination, may identify an individual e.g.. postcode, date of birth, etc.
Third Party	A person or organisation other than the main participants or organisation.

Contents

Introduction

The Information Governance Framework sets out the standards to be applied across the Health Board for managing information governance including the organisational arrangements, roles, responsibilities, and policies.

Information governance covers the framework of law and best practice to ensure information is managed in a confidential, secure, and consistent way. Particular focus is placed on the management of personal data and other confidential information to ensure it is handled legally, securely and effectively to provide the best possible service to our patients.

Policy Statement

The Health Board is committed to managing its information securely, legally and effectively in order to provide the best possible services to our patients. This framework provides clear guidance to staff around how information should be managed and outlines the accountability structures, governance processes, documented policies and procedures, staff training, and resources required to undertake this task.

Good information governance ensures that the Health Board is able to provide the right service, at the right time for the right people in an inclusive, open and accountable way that upholds the rights of individuals.

Scope

This framework applies to all Health Board staff and the following groups of people who work for or on behalf of the Health Board: committee chairs and members and remunerated expert advisors, agency workers, locums and contractors, secondees, students, volunteers and placement staff.

It applies to management and governance of all information across the Health Board with a particular emphasis on personal and confidential information. It applies to information held in both electronic and paper format and their associated systems.

Aim

The aim of the Information Governance Framework is to ensure that there is a clear structure in place for managing information governance across the Health Board and this is communicated to our staff and stakeholders. It will ensure that the Health Board is managing all information in an effective and efficient way and is meeting its legal and ethical requirements, including to safeguard the confidentiality and privacy of patients, staff and service users.

Objectives

- The Health Board is making the best use of the information it holds to provide the best possible service and care to patients.
- The Health Board is protecting personal information to ensure that the confidentiality and privacy rights of individuals are upheld.
- The Health Board is meeting its legal and statutory duties including in relation to the Data Protection Act / UK General Data Protection Regulations 2016 or any subsequent

legislation to the same effect, the Freedom of Information Act, the Human Rights Act and in upholding the common law duty of confidentiality.

- There is a strong senior oversight of information governance within the Health Board with a clear reporting structure to the Board.
- All Health Board staff understand the required standards for managing information and are clear about their individual responsibilities in this area.
- There are adequate policies, procedures and processes in place to meet the aims of the Information Governance Framework and these are applied consistently across the organisation.
- There is a clear structure for managing information risk across the organisation.

1. Roles and responsibilities

1.1 Chief Executive

The Chief Executive has overall responsibility for information governance and provides assurance through the Annual Governance Statement that risks relating to information are effectively managed.

1.2 Senior Information Risk Owner (SIRO)

The Director of Finance is the Health Board's SIRO and is the Executive representative to the board for Information Governance.

The SIRO:

- Leads and fosters a culture of good information governance across the Health Board.
- Ensures information governance compliance with legislation and Health Board policies.
- Has overall responsibility for managing information risk including information and cyber security.
- Chairs the Information Governance Sub-committee.

1.3 Deputy SIRO

The Digital Director acts as the Health Board's Deputy SIRO. The Deputy SIRO assists the SIRO in undertaking the responsibilities outlined above and acts as the deputy chair of the Information Governance Sub-committee.

1.4 Caldicott Guardian

The Medical Director and Deputy Chief Executive is the Caldicott Guardian for the Health Board. The Caldicott Guardian is responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing to promote high quality care.

The Caldicott Guardian:

- Leads and fosters a culture of good information governance across the Health Board with a focus on managing patient information.
- Upholds the standards around the safe and ethical use of patient information.
- Ensures that the Health Board is meeting its statutory requirements in relation to the management of patient information.
- Acts as the 'conscience' of the organisation and actively supports work to enable appropriate information sharing and advises staff on the options for lawful and ethical use of information.

1.5 Deputy Caldicott Guardian

The Associate Medical Director for Professional Standards acts as the Deputy Caldicott Guardian for the Health Board. The Deputy Caldicott Guardian assists the Caldicott Guardian in undertaking the roles and responsibilities listed above and, attends the Information Governance Sub-committee and subgroups to provide appropriate advice and support.

1.6 Data Protection Officer (DPO)

The Head of Information Governance is the Health Board's DPO, they facilitate the Health Board's compliance with its legal and ethical obligations in relation to the management of personal information by providing expert advice to the organisation around its duties and responsibilities.

The DPO:

- Advises the organisation of its requirements in relation to the Data Protection Act / UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect and other EU member state data protection provisions.
- Monitors the organisation's compliance with meeting the above and the organisation's policies and procedures including the assignment of responsibilities and training of staff and related audits.
- Collects information to identify what processing the organisation is undertaking.
- Provides advice in relation to Data Protection Impact Assessments (DPIA) (Privacy Impact Assessments) and monitors their performance.
- Cooperates with the ICO and acts as the contact point including ensuring that the ICO is consulted in the event that a DPIA shows there is a high risk in a processing activity being undertaken (or proposed to be undertaken).
- Has regard for and provides advice around risks associated with the processing of personal data.
- Provides advice, information and issues recommendations to the organisation or any organisation processing information on behalf of the Health Board.

1.7 Information Asset Owners

Each service area and major system that contains personal information is owned by a named Information Asset Owner. These individuals are accountable for the information held within their service area and understand how the information is held, used and shared. They work with the SIRO and the Information Governance Team to effectively manage information risk within their service area.

The Information Asset Owners promote a culture of good information governance within their service areas and disseminate information and key messages to their managers and staff.

1.8 Information Asset Administrators

Information Asset Administrators are named individuals within each service who assist the Information Asset Owners in the responsibilities outlined above.

1.9 The Information Governance Team

The Information Governance Team is responsible for providing expert advice and assistance to the organisation and for putting the requirements of the Information Governance Framework into practice. The Information Governance Team work with the DPO, SIRO, Caldicott Guardian, Information Asset Owners/Administrators and key staff across the Health Board to put in place all of requirements needed to ensure good information governance is in place across the Health Board:

- Staff training and awareness.
- Undertaking Data Protection Impact Assessments
- Managing the Information Security Incident procedure.
- Undertaking the Caldicott Principles into Practice Assessment and implementing the Action Plan.
- Developing and implementing the Data Protection, Confidentiality and other related policies.
- Developing appropriate information sharing agreements.
- Developing Data Processing Agreements and reviewing contract arrangements with third party organisations and suppliers.
- Managing the National Integrated Intelligent Audit System (NIIAS) to ensure appropriate access to patient records.
- Managing corporate subject access requests and advising the access to medical records and freedom of information teams.
- Developing the Health Board's information and cyber security compliance.

1.10 Access to Health Records Team

The Access to Health Records Team process requests for access to patient records in-line with the organisation's legal requirements and provide specialist advice and guidance about how patient health records are managed by the Health Board.

1.11 Corporate Office

The Health Board's Corporate Office manages requests and provides specialist advice in relation to the Freedom of Information Act 2000 and maintains the Health Board's publication scheme and disclosure log. The Corporate Office has responsibility for the management of corporate information in-line with the Health Board's policies and procedures.

1.12 Managers

Managers and supervisors have the following responsibilities:

- Ensuring information governance policies, procedures and guidance notes are read and understood by their staff.
- Ensure staff have completed their mandatory information governance training every two years via the ESR portal.
- Ensure staff understand their responsibilities in terms of patient confidentiality, in particular the fact that staff should never access a patient record or information unless it is required for a valid work purpose.
- Encourage the safe handling of information by their staff and report any concerns about practice to their Information Asset Owner or to the Information Governance Team.
- Report any information security incidents they are made aware of to the Information Governance Team immediately.
- Seek further guidance from the Information Governance Team in relation to any requests for information sharing that fall outside of providing direct patient care or an agreed information sharing process (unless in emergency situations).

1.11 Staff

All staff have the following responsibilities:

- Read and understand the Health Board's information governance policies, procedures and guidance notes and contact their manager if they require any clarification, advice and guidance.
- Complete their mandatory information governance training every two years via the ESR portal.
- Ensure they are handling personal information in-line with the Health Board's policies and procedures and report any concerns about practice to their line manager or the Information Governance Team.
- Report any information security incidents immediately to their line manager or to the Information Governance Team.
- Seek further advice from their line manager if they receive any requests to share information unless the request is part of a process already agreed with their line manager.
- Never access patient information or records unless they have a valid work reason for doing so and uphold patient confidentiality at all times.

2. Information asset and information risk management

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

An information asset is usually a set of information that can be identified as it is used for a specific purpose or function within the Health Board. Some examples of information assets:

- Patient complaint files,
- Staff disciplinary files,

- Child safeguarding referrals,
- Patient identifiable data held for a specific clinical audit,
- A patient waiting list in the A&E department,
- A database of contacts,
- An IT System that holds personal information on patients or staff.

The Health Board retains an information asset register for each service area. The asset register lists all personal information held and further details such as how it is stored, who it is shared with, the legal basis for processing and how long it is stored for.

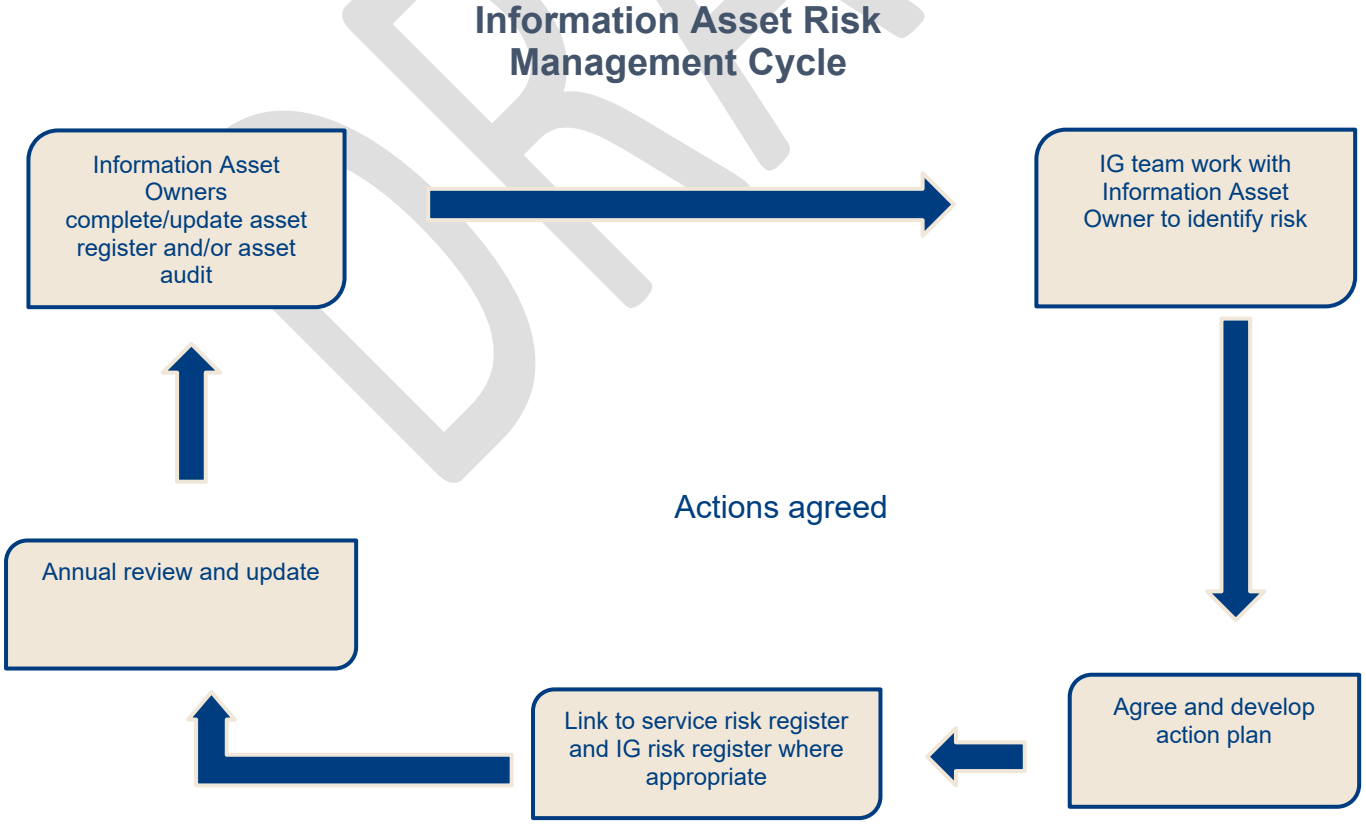
In addition to the asset register, the Health Board holds a detailed asset risk audit for its major systems that hold patient information. The risk audit has detailed information about how the information stored within the system is processed.

The Health Board maintains an asset risk register which identifies any information risk against an information asset and the actions that have been agreed to mitigate that risk.

Information Asset Owners are responsible for agreeing any actions to mitigate risk linked to their information assets and ensuring the actions are completed. Information Asset Owners can transfer any significant information risk onto their service risk registers.

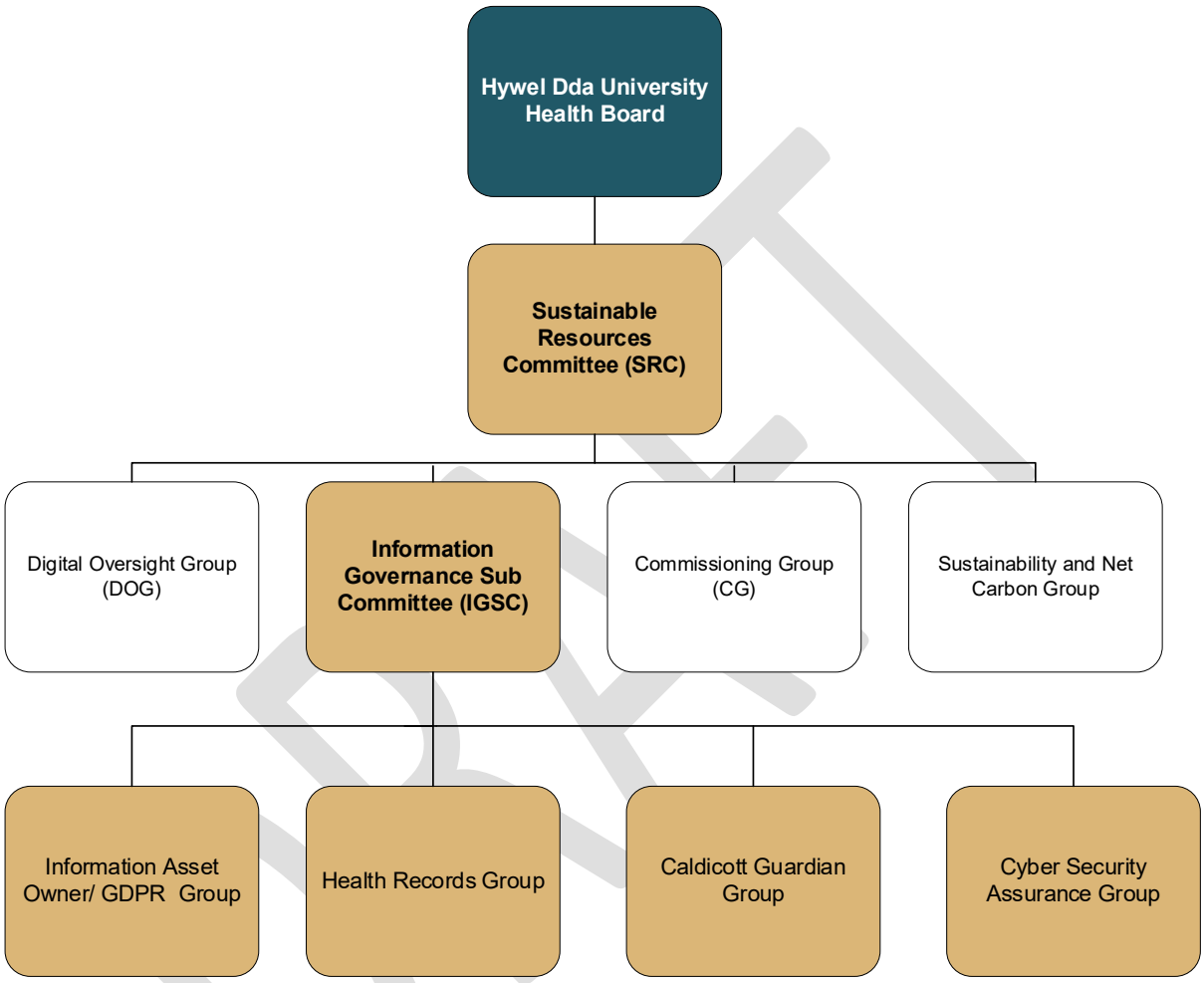
Any significant information risk that affects the organisation is added to the information governance risk register and is monitored through the Information Governance Sub-committee.

The diagram below outlines the information asset risk management cycle operated by the Health Board.



3. Governance structure

The Health Board has a clear governance structure to provide assurance to the Board that the organisation is complying with its statutory requirements and guidance and best practice in relation to information governance practice.



The Information Governance Sub Committee (IGSC) is responsible for ensuring the Health Board is compliant with information governance legislation and information handling requirements and good practice standards. The committee oversees and influences the development of Information Governance and Security across the Health Board and with third party suppliers and contractors.

The Sub-committee oversees the following key areas:

- Information and Cyber Security (Inc SIRO related issues)
- Information Sharing Protocols
- Contracts, partnership and third party and supplier agreements
- Confidentiality and Data Protection

- Freedom of Information
- Subject Access Requests
- Records Management
- Information Quality Assurance
- Risk Management and Incident Management
- Data Protection Impact Assessments

The Information Governance Sub-committee (IGSC) provides assurance to the Board via the Sustainable Resources Committee which it reports to on a bimonthly basis. The IGSC receives regular assurance reports from its sub-groups that detail the work undertaken and reporting significant risks.

The following sub-groups report to the Information Governance Sub-Committee and oversee the day-to-day work in relation to key policy areas:

- **Information Asset Owners/General Data Protection Regulation (IAO/GDPR) Group** – to take forward the UK GDPR work plan, establish Information Asset Owners across the organisation and to develop an information asset register.

- **Health Records Group** – to discuss and resolve risk and issues affecting the health record and its users and to provide clear leadership in the promotion of effective health records management. To support the development of a Health Board wide integrated records management system, including storage, security arrangements and the move towards an electronic patient record (EPR), providing expert advice and guidance.

- **Cyber Security Assurance Group** - to ensure there is robust governance and assurance around how the organisation is managing and reporting its cyber security risks, incidents and ongoing work in accordance with regulations.

4. Information governance policies and procedures

The IGSC has responsibility for recommending policies and procedures relating to information governance to the Sustainable Resources Committee for approval on behalf of the Board.

All policies are available to staff via the Health Board's policies and procedures information governance intranet page: Information Governance Policies and Procedures

5. Information governance training and awareness

Current approach to information governance training

The Health Board is currently adopting the following approach to staff information governance training:

- The Health Board offers a mandatory e-learning information governance module that must be completed by all staff every two years.
- The Information Governance Team undertakes mandatory online training for any staff that have accessed their own record or a family member's record without a valid work reason for doing so.

- The Information Governance Team also undertakes mandatory online training for any staff member or team where there has been an information security incident, personal data breach or near miss.
- Managers and staff can request additional training from the information governance team if they have identified a need within their service area.
- The Information Governance Team undertake online or classroom-based information governance training for key staff groups if required e.g. estates staff, nursing staff, clinical staff etc.

Current approach to awareness raising

The Information Governance Team undertake a number of awareness raising activities which are planned through an annual communications plan. Some examples of activities are provided below:

- Producing and disseminating information leaflets, posters and FAQs.
- Running Information Governance drop-in sessions.
- Running a Data Protection/Information Governance Awareness Day/Week.
- Using global e-mails, pop-ups, newsletters and messaging to provide information to staff.
- Information Governance Officers audits or visits to hospital sites.

Monitoring of training compliance

Information Governance mandatory training compliance is reported on and monitored through the IGSC on a bimonthly basis.

Information Governance Training and Awareness Strategy

The Health Boards Information Governance Training and Awareness strategy plans to develop a strategic approach to improving information governance training and awareness within the current resources available. The strategy will look at the following key areas:

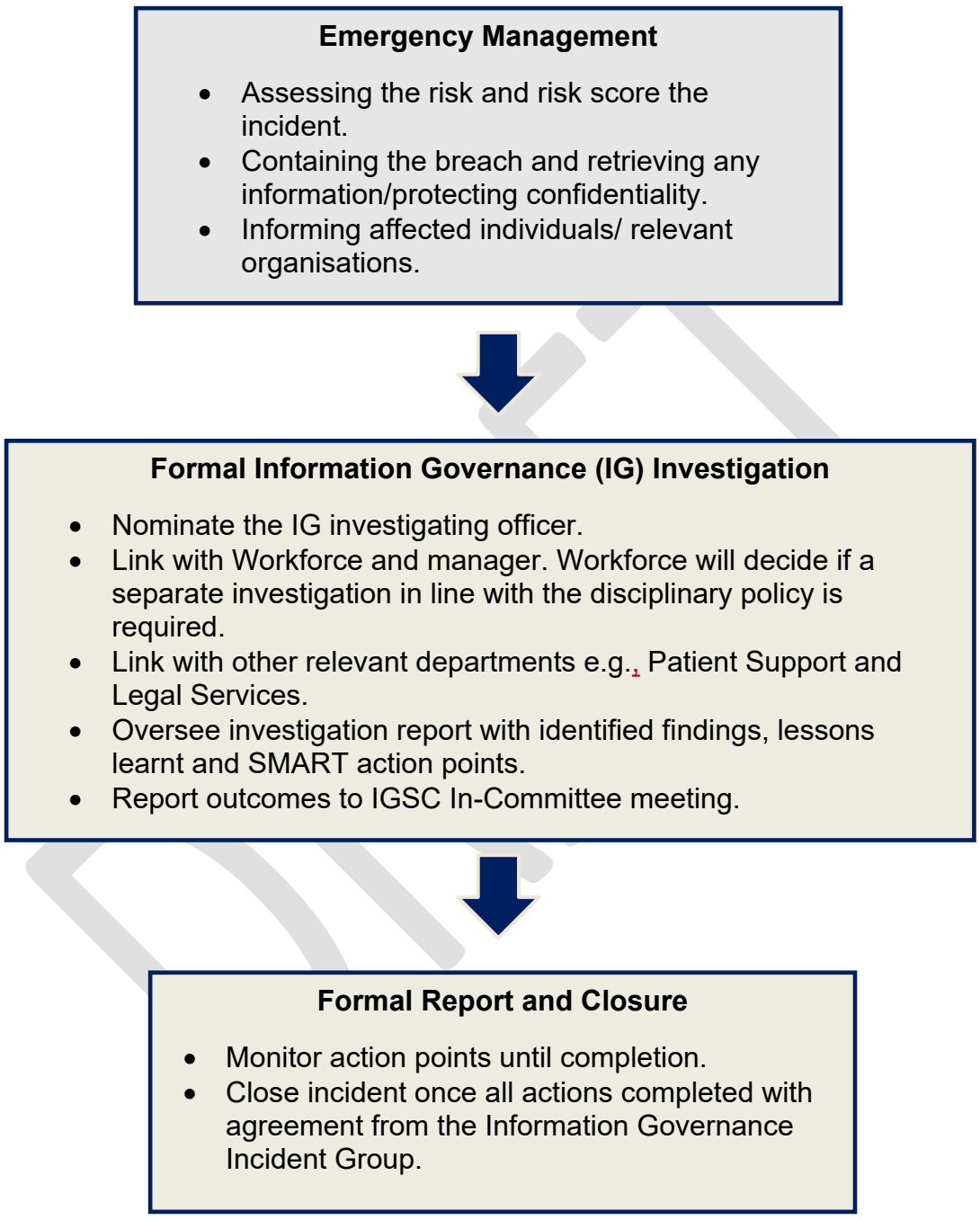
- Improving the completion rate for mandatory information governance training.
- Undertaking a training needs analysis to ensure that resources are concentrated in the right areas.
- Developing an on-line resource of easy read guides for managers and staff that cover key information governance areas.
- Improving the information provided to new staff at induction.
- Identifying areas where training is already taking place with key staff groups and putting information governance onto the agenda.

6. Information governance incident management

The Health Board has an Information Governance Incident Procedure that provides clear guidance to staff about what to do if they become aware of an information security incident. All incidents must be reported to the Information Governance Team immediately through DATIX.

6.1 Incident reporting process

The following process is followed for the management of all information security incidents:



7. Reporting structures

The Information Governance team discuss all Incidents in the IGSC In-Committee meeting. The members of the In-Committee meeting are the decision-making group in relation to all information security incidents. The meeting takes place on a bi-monthly basis as part of the IGSC In-Committee meeting and be chaired by either the Deputy SIRO or DPO.

8. Managing third-party access to information

Third party supplier agreements and contracts

The Health Board has a Third-Party Supplier Security Policy which outlines the process that must be followed before information is shared as part of any agreement or contract with an outside organisation.

The policy is linked to the Health Board's procurement process and ensures that full assurance is provided to the Health Board that a third-party supplier has the appropriate security and technical measures in place to protect the Health Board's personal information.

The Health Board ensures that any contract or agreement entered into with a third-party supplier has the appropriate contract or data processing agreement in place that outlines the information governance requirements prior to any information being shared.

Information sharing with other organisations

Information sharing is managed in accordance with the Health Board's data sharing protocols to ensure information sharing is managed in line with the organisation's legal duties and is carried out in a safe and secure way.

Information is shared on a strictly 'need to know' basis with only the minimum amount of information required being shared.

9. IT, cyber-security and business continuity

The Health Board applies a comprehensive set of controls to the internal network to ensure resilience and disaster recovery in the event of a temporary or total loss of the network and/or key IT systems.

Business continuity plans are in place for key electronic systems and a programme of development is being implemented through the Information Asset Owners Group.

The Health Board is currently working towards compliance with The Network & Information Systems Regulations (NIS-R), and have developed a programme of work over the next 24 months. The Cyber Security Programme is made up of 15 workstreams that cover remediation activities required to reduce cyber security risk and comply with the NIS-R.

10. Monitoring and review

The key areas of information governance and their related action plans are monitored through regular reporting to the Information Governance Sub-committee. These action plans form the basis of the annual work plan for the Information Governance Team.

Regular audits are undertaken by the shared services audit team with actions identified and agreed by the service lead. Progress against these actions is monitored through the Information Governance Sub-Ccommittee and, any areas of the information governance framework that are

considered to be of limited assurance and below are reported to the Audit and Risk Assurance Committee (ARAC) which reports directly to the Board.

The Welsh Audit Office carry out regular audits of the Health Board's information governance practice and, recommended actions are built into the Information Governance Team's work plan and are reported through the Information Governance Sub-Ccommittee.

The Information Governance Framework is reviewed every two years through the Information Governance Sub-committee.

11. Who to contact:

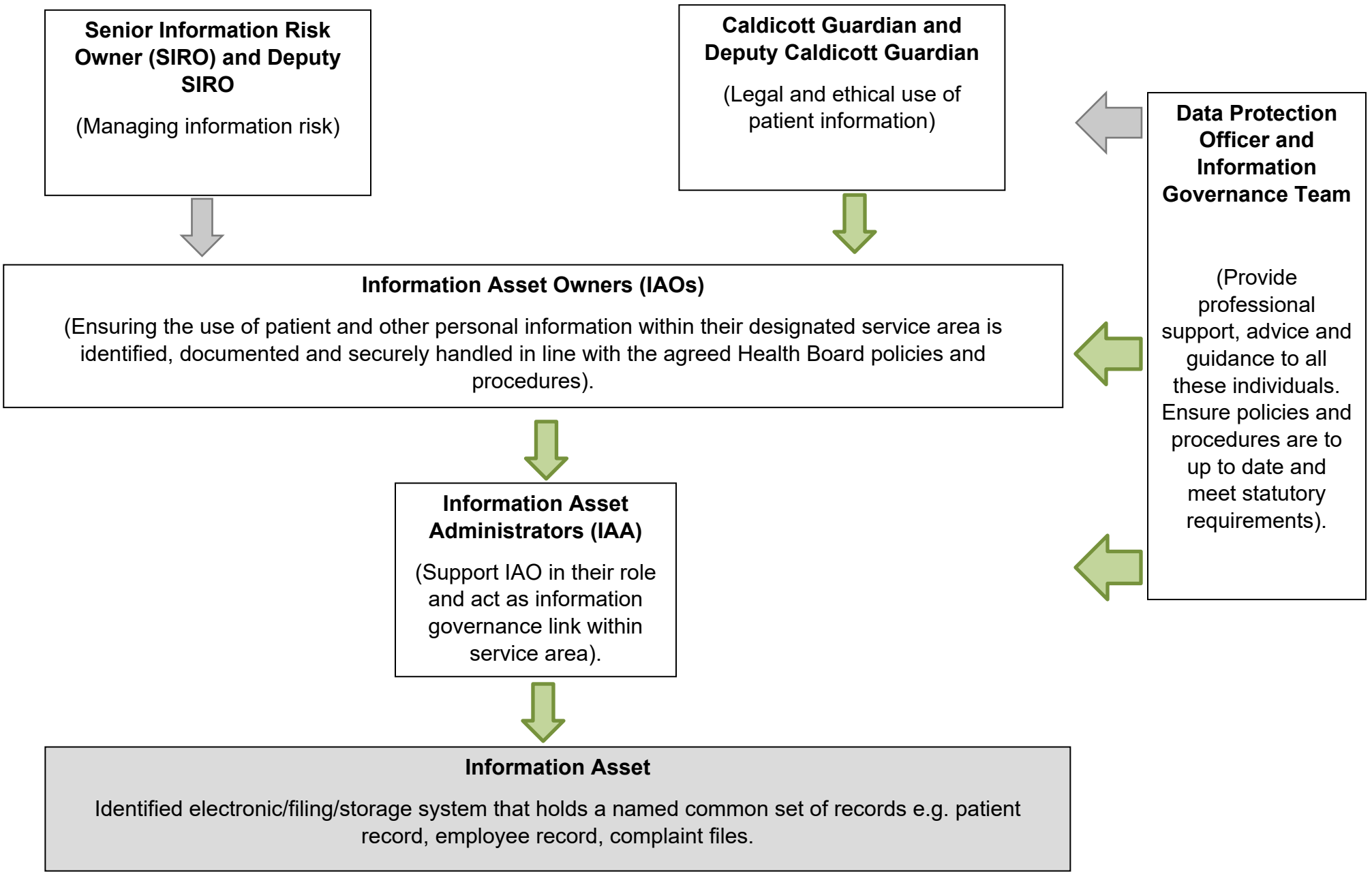
Should you have any queries in relation to this policy please email the Information Governance Team at: Information.Governance3@wales.nhs.uk, alternatively, you can contact:

Data Protection Officer (DPO) at: DPO.HDD@wales.nhs.uk,

Senior Information Risk Officer (SIRO) at: SIRO.HDD@wales.nhs.uk

Caldicott Guardian at: CaldicottGuardian.HDD@wales.nhs.uk

Appendix 1 – Responsibility for the management of Information Assets within Hywel Dda University Health Board



SUMMARY EQUALITY IMPACT ASSESSMENT – 238 – Information Governance Framework

Organisation:	Hywel Dda University Health Board

Proposal Sponsored by:	**Name:**	Patrycja Duszynska
	Title:	Head of Information Governance
	Department:	Digital Services

Policy Title:	Information Governance Framework - Review March 2023

Brief Aims and Objectives of Policy:	The Information Governance Framework sets out the standards to be applied across the Health Board for managing information governance including the organisational arrangements, roles, responsibilities and policies. The aim of the Information Governance Framework is to ensure that there is a clear structure in place for managing information governance across the Health Board and this is communicated to our staff and stakeholders. It will ensure that the Health Board is managing all information in an effective and efficient way and is meeting its legal and ethical requirements, including to safeguard the confidentiality and privacy of patients, staff and service users. This will be achieved through the following objectives: • The Health Board is making the best use of the information it holds to provide the best possible service and care to patients. • The Health Board is protecting personal information to ensure that the confidentiality and privacy rights of individuals are upheld.

	• The Health Board is meeting its legal and statutory duties including in relation to the Data Protection Act /General Data Protection Regulation 2016 or any subsequent legislation to the same effect, the Freedom of Information Act, the Human Rights Act and in upholding the common law duty of confidentiality. • There is a strong senior oversight of information governance within the Health Board with a clear reporting structure to the Board. • All Health Board staff understand the required standards for managing information and are clear about their individual responsibilities in this area. • There are adequate policies, procedures and processes in place to meet the aims of the Information Governance Framework and these are applies consistently across the organisation. • There is a clear structure for managing information risk across the organisation.

Was the decision reached to proceed to full Equality Impact Assessment?	**Yes**	**No√**
	The policy provides an overarching framework based on legislation in relation to ensuring that information within the Health Board, including sensitive personal information is collected, used and stored appropriately. Adherence to the policy should ensure that no individual is adversely impacted by the implementation of this policy in relation to any protected characteristic/s and that their human rights are upheld. The current version constitutes a review including changes to the staff job titles, changes to reporting committee. No complaints in relation to equality, diversity or human rights have been received since implementation of previous policies.	

	It is not anticipated that changes made with this review will have an adverse impact on protected groups. A search of similar policies elsewhere indicated a neutral impact: https://www.bing.com/search?q=information+governance+framework+nhs+equality+impact+assessment+&qs=n&form=QBLH&sp=-1&ghc=1&pq=information+governance+framework+nhs+equality+impact+assessment+&sc=0-64&sk=&cvid=A55274F0E20A4669A6EE6115C9284544	
If no, are there any issues to be addressed?	**Yes**	**No√**

Is the Policy Lawful?	**Yes √**	See references to legislation within policy

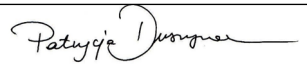
Will the Policy be adopted?	**Yes √**	The policy is an existing policy, fully reviewed and updated in line with current legislation

	If no, please record the reason and any further action required:

Are monitoring arrangements in place?	**Yes √**	
	Any complaints received in relation to equality, diversity and human rights will be addressed on an individual basis and appropriate action taken.	

Who is the Lead Officer?	**Name:**	Sarah Bevan
	Title:	Information Governance Manager
	Department:	Information Governance / Digital Services
Review Date of Policy:	Three yearly or sooner if required	

Signature of all parties:	**Name**	**Title**	**Signature**
	Jackie Hooper	Senior Equality and Diversity	3 May 2018

		Officer, Strategy, Policy and Advice	
	Sarah Bevan	Information Governance Manager	 **Review March 2023**
	Patrycja Duszynska	Head of Information Governance	 **Review March 2023**
	Alan Winter	Senior Diversity & Inclusion Officer	25/6/2023

Please Note: An Action Plan should be attached to this Outcome Report prior to signature

N/A