Enw y Grŵp/Is-Bwyllgor: Name of Group:	**Information Governance Sub-Committee (IGSC)**
Cadeirydd y Grŵp/Is-Bwyllgor: Chair of Group:	**Huw Thomas, Executive Director of Finance**
Cyfnod Adrodd: Reporting Period:	**13 April 2023**

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

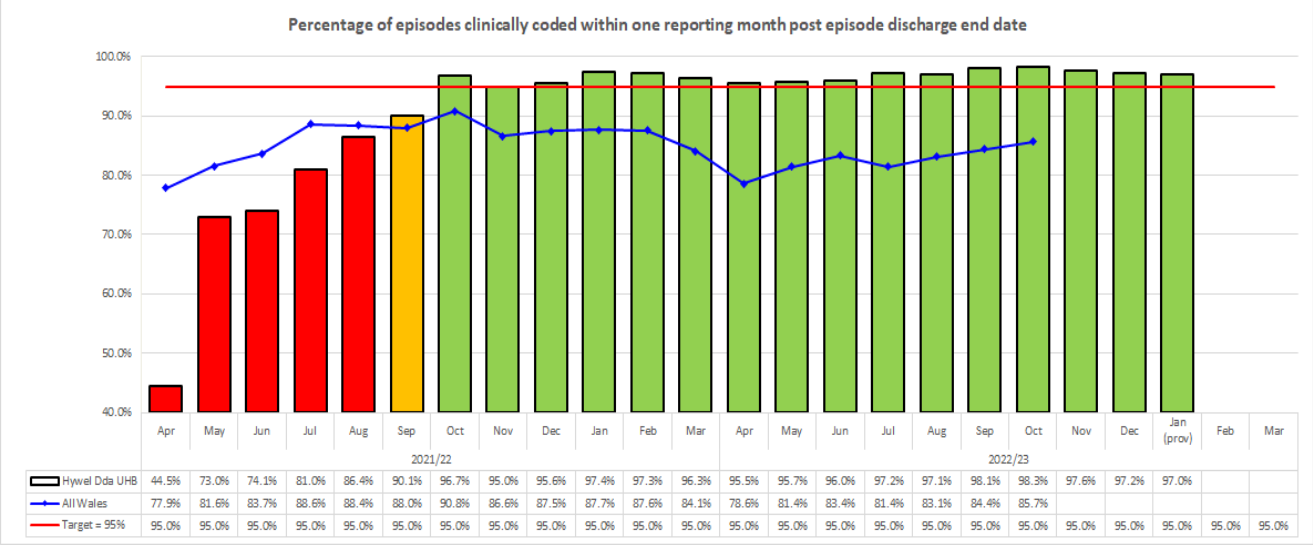
Policies and Procedures:

The Sub-Committee approved the following policies for approval by the Committee:

- 320 – Acceptable Use of Information and Communication Technology Policy – approved to be passed to the Committee for approval, attached at Appendix 1.
- 240 – Informatics Procurement & Request Procedure – approved to be passed to the Committee for approval, attached at Appendix 2.

Clinical Coding Update

The Sub-Committee received a report, which provided an update on the clinical coding position for the Health Board. Health Board performance has achieved the 95% target for the last 15 months, with latest performance for January 2023 provisionally at 97.0%.



The current backlog position for 2022/23 activity shows that the Health Board has 98.6% of episodes from April to January 2023 coded and is therefore on track to achieve the 98% for the end of the financial year by continuing on this trajectory.

The Sub-Group was also informed on development work that is being undertaken by the clinical coding team, namely:

- **Coding of A&E Attendances** - The further work with 3M, which was focusing on the potential to clinically code some of the longest waiting patients in the Health Board Emergency Departments. This will give the Clinical Coding team the tools to allow us to clinically code some of the A&E activity across the Health Board. The plan would be to look at those patients staying over 24 hours in an emergency department who are not

admitted to a ward in the first instance before potentially moving onto those who are less than 24 hours to improve the intelligence around patients within ED providing an enhanced dataset for the Transforming Urgent Emergency Care Programme.

- **Robotic Process Automation (RPA)** - A process excellence workshop was held with representatives of Northampton General Hospital Trust to understand the workflow in the clinical coding team for Endoscopy coding. The workshop was attended by the Clinical Coding Manager, both supervisors and five clinical coders who have provided as much detail as possible to help the team from Northampton to assess the best way we can handle the process for a robust automation solution for Endoscopy coding. Endoscopies have been targeted as a good source of electronic information, which RPA is predominantly based on. There is potential to code 9,500 episodes this way to free up the clinical coders time to assist in coding of other things, such as A&E.
- **GIRFT (Getting it right first time)** - The Clinical Coding Manager has been involved in the first Health Board internal Gynaecology Task and Finish Group regarding the national Gynaecology GIRFT report, which was held on 20 March 2023. The Clinical Coding Manager has also attended the first Sub Working Group to improve Gynaecology Data Collection for Gynaecology meeting on 24 March 2023, which involved other clinical coding managers across Wales, as well as representatives from the Gynaecology teams across different organisations in Wales. This is looking at how we can look to improve the clinical documentation for Inpatient activity in addition to improving the process to code procedures that occur in an outpatient setting.

Information Quality Assurance (IQA) Data Quality
The Sub-Committee received an update on data quality within the Health Board specifically around a deep dive into Clinical Decisions Unit activity. The results of the work have been fed back to the service.

The Sub-Committee also received an approach to prioritise the data quality issues, by applying a "score". The matrix will be used for any new pieces of work moving forward and will also be used as an escalation process to ensure that actions and recommendations identified in IQA reports are being looked at and owned through to completion.

HDdUHB's Corporate and Medical Records Storage Assurance Report – Update
The Sub-Committee received an update on the current audit of storage facilities across the Health Board. The IG team contacted the Withybush Senior Team to discuss several storage containers at the rear of the hospital and the audits have taken place and actions have been passed to the Withybush Senior Team. The IG team is now contacting the remaining areas of Pembrokeshire County (i.e. South Pembrokeshire Hospital, Tenby Cottage Hospital, and other sites) to undertake similar audits.

Information Commissioner Office (ICO) Notifications
Since April 2022, there have been five occurrences when a notification to the 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	1	0	1	0	1	0	0	0	1	-	-	1	5
Closed	-	-	-	-	-	-	-	-	-	-	-	-	0
Total	1	0	1	0	1	0	0	0	0	0	0	0	5

IG Annual Report (2022 – 2023)
A separate report will be prepared for presentation to the June 2023 Committee meeting of the Sustainable Resources Committee.

IG Activity Report, Quarter 4 (January – March 2023)

- **National Intelligent Integrated Audit Solution (NIIAS) Monitoring** – All alerts have decreased from the previous quarter, with 19 incidents of staff accessing their own record, 19 staff accessing a family record, and one person accessing a person of interest.

- **Information Security** – Figures show a decrease compared with the previous quarter however, a significant increase compared with the first two quarters. This was as a result of the new version of Forcepoint being rolled out that had exceptions removed resulting in legitimate websites being blocked as well as a further Phishing Email exercise, where emails were sent to a limited number of Health Board's employees that contacted the service to report.

- **Subject Access Requests** – Requests for access to records continue to increase. Third Party Requests Q3 484 with Q4 reaching 622. Health access to records Q3 308 with Q4 reaching 382. The Corporate access to records requests decreased during Q4 to 6.

- **Personal Data Breaches** – Breaches reported to Information Governance have increased further this quarter to 202. There has been a significant increase in the category Unauthorised access / disclosure however 30 of these 45 incidents were captured having undertaken new monitoring of personal identifiable information (PII) being sent to personal email address that were captured via MailMarshal. Additionally, the Information Governance team also considered 269 incidents reported on DATIX to have no IG concerns. One Personal Data Breach was reported to the Information Commissioner's Office, following a report from a patient that their confidentiality had been breached.

- **Training Compliance** – Compliance is gradually increasing however, Q4 does not include the statistics for March 2023, as they were unavailable at the time of writing this report. The current training compliance is 78.6%.

Digitisation of Health Records
The Sub-Committee received an update in regard to the digitisation project and the scanning of non-active patient records, including some of the early decisions made and progress to date. The Sub-Committee thanked the reporting officers for the considerable amount of work that has been undertaken and the significant progress made in regard to the digitisation of patient records.

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

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

Approval of the following policies:

- 320 – Acceptable Use of Information and Communication Technology Policy

- 240 – Informatics Procurement & Request Procedure

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 / NISR
- Caldicott Register to be returned to the IGSC meetings
- Digital / IG Policies and Procedures

Dyddiad y Cyfarfod Nesaf:
Date of Next Meeting:

8 June 2023

Acceptable Use of Digital Services Policy

Policy information

Policy number: 320

Classification: Corporate

Supersedes: Previous versions

Version number: 3

Date of Equality Impact Assessment:
Detail date of EqIA

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 purpose of this policy is to provide guidance to users regarding the acceptable and unacceptable use of Health Board Digital systems and networks and including: defining what is acceptable use, including personal use; defining what is unacceptable use, including personal use during working time and accessing of indecent, obscene or offensive material; defining the consequence of unacceptable use.

The policy explains how the Health Board has put in place: mechanisms to monitor users and their usage; mechanisms that prevent access to indecent, obscene or offensive material; ensures that breaches of this policy are dealt with quickly and in line with disciplinary procedures where necessary.

Scope:
This policy applies to all employees of the Health Board, volunteers, other NHS and health organisations, and other contracted staff; having the facility to use the Health Board's e-mail and

internet services, plus anyone granted access to the Health Board network whilst engaged in work for the Health Board at any Health Board occupied location, and/or on any Health Board owned or Health Board approved computer asset.

This policy applies to all users of Digital Services in relation to:

- The use of digital equipment.
- The use of digital communication tools.
- Digital systems connected directly or remotely to the Health Board NHS managed network or used on the Health Board's premises.

To be read in conjunction with other Digital Policies and Procedures.
201 – AW Disciplinary Policy – opens in a new tab

Owning group:
Information Governance Sub-Committee
13/04/2023

Executive Director job title:
Director of Finance

Reviews and updates:
Version 1 – new policy 28.91.2013
Version 2 – revised and amended 21.5.2018
Version 3 – full review

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

Glossary of terms
DHCW – Digital Health and Care Wales
DCP - Discretionary Capital Programme
ICT – Information & Communications Technology

Contents

Aim

The aim of this policy is to ensure all users of Health Board services do so in a safe and secure manner ensuring compliance with relevant legislation.

Objectives

The objectives of this policy are to: -

- Clarify Health Board policy regarding acceptable and unacceptable use of Digital services, and Health Board network access.
- Reduce or avoid security threats by increasing awareness and disseminating good practice.
- Cease the copying/distribution of copyrighted materials.
- Encourage effective use of Health Board resources.
- Protect the Health Board against potential liability.

Scope

This policy applies to all employees of the Health Board, volunteers, other NHS and health organisations, and other contracted staff; having the facility to use the Health Board's e-mail and internet services, plus anyone granted access to the Health Board network whilst engaged in work for the Health Board at any Health Board occupied location, and/or on any Health Board owned or Health Board approved computer asset.

This policy applies to all users of Digital Services in relation to:

- The use of digital equipment.
- The use of digital communication tools.
- Digital systems connected directly or remotely to the Health Board NHS managed network or used on the Health Board's premises.

Becoming and Authorised User

Every member of staff or contractor who requires access to Digital systems must complete the relevant online form available on the Digital Services Portal to request an account with the necessary access to Digital systems. If the account is approved by their line manager, the user will be set-up with a username and password by the Digital Service Desk.

In the unlikely event of the application being turned down the staff or contractor will be contacted to communicate the reasons for rejection. Access to Digital systems will only be through the following means:

- Health Board NHS managed network which is protected by perimeter firewalls, anti-virus software and content filters.
- Authorised remote access using Cisco Anyconnect, Citrix Gateway, or Microsoft Office 365.

Acceptable Use

Access to Digital systems is primarily for business related purposes. Personal use is permitted provided this does not interfere with the performance of your duties, those of other staff or contractors or the business of the Health Board in general. Personal access to Digital systems can be limited or denied by your manager. Staff and contractors must act in accordance with Health Board Policy.

However, there can be no expectation of the privacy of personal e-mails. In certain circumstances and following the processes contained in the Information Commissioner's code of practice on staff data, the organisation may, in a proportionate manner, view personal e-mails as legislation or the Health Board's Disciplinary procedures permit. In such circumstances, the Regulation of Investigatory Powers Act (2000) and the Lawful Business Practices Regulations (2000) confirms that the organisation's responsibilities may prevail over a member of staff's individual rights to confidentiality of correspondence. The Health Board reserves the right in these circumstances to view the content of an individual's mailbox.

Unacceptable Use

This policy sets the common minimum standards for the acceptable use of Digital systems and services. Set out below are examples of activities and uses which are specifically excluded. The list is not comprehensive and is divided into two sections ("Unacceptable" and "Forbidden") to help highlight the most serious activities. The consequences of undertaking any of the activities listed below (or other instances) will be determined through the normal disciplinary procedures. All such activities are serious and are likely to be viewed as misconduct. It is likely that undertaking a forbidden activity, or repeating an unacceptable activity, will be viewed as gross misconduct.

Any unacceptable use will be reported as per the Information Governance incident procedure, and it is the responsibility of the investigating officer to ensure that the matter is dealt with in line with current Information Governance and Digital policies and procedures. This may result in a full enquiry that could result in disciplinary action being taken and access of the staff or contractor involved may be suspended pending the enquiry conclusion at which point it may be terminated.

Unacceptable use of Digital systems provided by the Health Board are shown below:

- Spending more than permitted amounts of working time making personal use of the internet, e-mail, and other Digital Systems and services.
- Transmitting, downloading or storing any material such that this infringes the copyright of the owner.
- Purchasing goods or services or entering any contract via the Internet or any other Digital system on behalf of the Health Board without the necessary authority and not in accordance with the Health Board's standing financial instructions.
- Business advertisements or trading, i.e., sale of any goods purchased with the sole intention of making a profit.
- Using an unauthorised electronic communication mechanism for the transmission to a third party of personal identifiable data or confidential material concerning the activities of the Health Board.
- Using unauthorised external email accounts for Health Board activities such as Outlook.com or icloud.com.
- Using cloud-based services where Health Board confidential data or person identifiable information could be stored outside of the European Union or European Economic Area.

- Unauthorised redistribution of email.
- Sending or forwarding spam emails.
- Making your Cymru or any other system user name and password (also known as a 'user account') available for other people to use on your behalf.
- Accessing another individual's data, Digital systems, or service without appropriate authorisation.
- Deliberately creating, storing, or transmitting information which infringes the Data Protection Act/General Data Protection Regulations 2018 or any subsequent legislation to the same effect.
- Knowingly allowing the use of Health Board's Digital resources by unauthorised third parties.
- Disabling, altering bypassing, or circumventing any measures put in place by the Health Board to maintain the safe and secure operation of Digital systems and services.
- Failing to follow Health Board advice on how to protect, store, transmit, share, and access sensitive information.
- Failing to purchase and dispose of Digital systems and services in line with Health Board policies.
- To load software / apps for which no legitimate licence is held or software / apps that are unapproved.
- Unauthorised removal or relocation of hardware, software, documentation, or media associated with the Health Board's Digital systems.

Forbidden uses of Digital systems provided by the Health Board are shown below:

- Using another person's identity to appear to be someone else.
- Attempting to gain or facilitate unauthorised access to a computer system or information.
- Attempting to or deliberately corrupting, destroying, or denying access to another user's e-mail, data files, information, Digital system, or service.
- Deliberately accessing, viewing, receiving, downloading, sending, or storing material:
    - with pornographic, offensive, obscene, or indecent content.
    - related to criminal skills or terrorist activities.
    - that promote or encourage discrimination, racism, or intolerance.
    - that facilitates illegal activity in the UK or the host country.
    - that is illegal in the UK or the host country.
    - that is defamatory, threatening, harassing, offensive or abusive.
    - that will, or is likely to, bring the Health Board and its staff into disrepute.
    - that is known to be infected with a virus, worm, Trojan or any form of malicious software or code; that infringes the privacy and data protection rights of individuals.
    - that could endanger the health and safety of any other individual.

The Use of the Organisations Name

If staff or contractors join an Internet forum, they are expected to conduct themselves in an honest and professional manner. Individuals are responsible for what they write and should be always courteous and inoffensive. Staff and contractors are reminded to carefully consider whether to contribute to an Internet forum. Unless currently authorised to do so, staff and contractors are not permitted to write or present views on behalf of the Health Board. For example, staff and contractors cannot join an Internet forum in the name of the Health Board, nor can they design a web site and publish it under the name of the Health Board.

Staff and contractors are also reminded to carefully consider whether to distribute or publish their Health Board e-mail address (such as when registering on third-party websites) as this may lead to the staff or contractors mailbox being targeted by spam (commercial unsolicited e-mail) and phishing (fraudulent e-mails designed to aid identity theft) attacks or the Health Board's systems being subject to attacks designed to prevent legitimate access and cause general disruption (Denial of Service).

E-mails sent using the Health Boards e-mail system include the organisations name and may be held to represent the Health Board and its values. In exchanges of e-mails, staff could accidentally tarnish the image of the Health Board and this policy aims to assist with the understanding of e-mail good practice to avoid this. Use of Digital systems in such a way as to expose the Health Board to risk of claims for defamation is prohibited.

Unintentional Breaches of Digital Security

If staff or contractors find themselves unintentionally viewing material, which may be inappropriate, they must make all reasonable attempts to close the application concerned immediately and inform the Digital Service Desk. A note of this unintentional access will be recorded, and any content filtering rules modified where necessary to ensure that further unintentional access does not take place.

Acceptable Network and System Usage

It is the responsibility of all users to ensure that they adhere to the guidelines laid down in this policy. Before a new user can be allocated an account, they must have signed, understood and agreed to the terms of this policy, indicating that they are aware of their responsibilities. A record of which will be retained by the Informatics Department.

The instructions contained in the policy are special restrictions in force with regard to the Health Board related computer systems and network and, are clarifications or additions to the normal security measures in force within the Health Board. All usual security precautions must be taken in addition to these specific requirements.

Responsibilities

Executive Directors

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

Executive Directors must: -

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

Digital Services

Digital Services will be responsible for maintaining the hardware and software components of the Digital and communications infrastructure and, implementing all necessary technical and physical security controls; in summary the department will: -

- Ensure the availability of Digital services and their supporting infrastructure.

- Managing the security and integrity of data, via anti-virus, mail content, web filtering and content, and anti-spam products.
- Managing and monitoring the e-mail quarantine area and releasing appropriate messages.
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.
- Maintaining technical and engineering safeguards in accordance with this Policy and according to the allocated resources.
- Advise Executive Directors and Line Managers on matters relating to Information security.

Heads of Department / Line Managers

- Ensure all staff read, understand, and abide by this policy and any associated policies.
- Ensure that awareness to this policy is highlighted at their local induction programme.
- Monitoring staff compliance to the policy.
- Monitoring staff time spent on personal use of Digital services and systems.
- Instigating further investigations arising out of suspected misuse.
- Acting re misuse in accordance with the Health Board's 201 – All Wales Disciplinary Policy (opens in a new tab).
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.
- Ensure the Digital Service Desk is made aware of new starters, users changing roles and leavers of the Health Board using the appropriate electronic forms on the Digital Services Portal.

All Staff

All staff, permanent, temporary, or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality and understand they are required to comply with this policy. Failure to comply with this policy may result in disciplinary action being taken.

Staff and contractors who are authorised to access Digital systems have a responsibility to ensure that any usage conforms to policy and legislation relating to Digital security, confidentiality, and data protection.

Digital systems are a business tool that should be treated like any other tool in the workplace. Staff and contractors should be aware that their manager and colleagues may need to gain access to an individual's Digital systems under certain circumstances. Staff and contractors are therefore advised to carefully consider the use of Health Board provided Digital systems for personal use.

Digital systems are a shared resource, and each user has responsibility to learn how to use them appropriately.

Staff must:-

- Comply with this policy and associated guidelines.
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.

Training

All staff will be made aware of this procedure through a communications plan and availability to view on the Health Board Intranet site.

Targeted communications will also be undertaken to the groups identified in the Responsibilities Section.

Support will be provided by Digital Services Department as required to support Health Board staff in ensuring they meet the requirements of this policy.

Digital Procurement and Requests Procedure

Policy information

Policy number: 240

Classification: Corporate

Supersedes: Previous versions (previously named Informatics Procurement & Request Procedure)

Version number: 3

Date of Equality Impact Assessment:
Detail date of EqIA

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:
Hywel Dda University Health Board is committed to ensuring all Digital purchases align with both local and national strategies and that they represent value for money to public funds.

This procedure sets out a series of steps to follow to ensure all Digital purchases meet the requirements above and satisfy both the technical infrastructure and security requirements of the Health Board.

The procedures in this document are to be followed to ensure all requests for new Digital projects follow the correct governance and assurance arrangements before being committed into the Digital Operational Plan.

Scope:
This procedure covers everyone that is employed by Hywel Dda University Health Board who may request Digital services. The definition of Digital includes the following services: -

- Telecommunications (Telephones, paging and mobiles).
- Desktop Equipment (PC's, printers, scanners, projectors, and other peripherals).
- Mobile Equipment (Tablets, Android / Apple devices, carts).
- Medical equipment which connects to the Health Board network or includes software which needs to be assessed from an Information Governance / Cyber Security perspective.
- Audio-Visual equipment.
- Equipment to support health & safety assessments in relation to the use of display screen equipment regulations.
- Office moves and refurbishments.
- New Builds.
- Requests for new Digital Services.

To be read in conjunction with:
Digital Health Strategy (opens in a new tab)
837 – All Wales Information Security Policy (opens in a new tab)
Health Board's Standing Financial Instructions (opens in a new tab)
Standing Orders (opens in a new tab)
Capital Investment Procedure (opens in a new tab)

Owning group:
Information Governance Sub-Committee
13/04/2023

Executive Director job title:
Director of Finance

Reviews and updates:
Version 1 – new policy 6.9.2011
Version 2 – revised and amended 26.2.2017
Version 3 – full three yearly review

Keywords
Digital procurement procedure

Glossary of terms
DHCW – Digital Health and Care Wales
DCP - Discretionary Capital Programme
ICT – Information & Communications Technology

Contents

1. Aim

It is the responsibility of the Digital Senior Management Team to oversee the implementation of the Digital Strategy, including commissioning additional developments and resources as required. This document sets out the method by which Digital and System procurements, new Digital projects, adhoc departmental moves and changes as well as enhancements to existing systems will be approved, allocated resources, and ensuring that appropriate governance and assurance is sought.

The procedure for gaining approval for Digital initiatives is dependent on the context of the project. If the project is: -

- **Procurement of standard ICT equipment** (purchasing of standard hardware, software, mobile phones / smartphones, and peripherals such as printers and scanners) should follow the "Procurement of Digital Equipment" procedure outlined in section 4.
- **Adhoc departmental moves and changes** should follow the 'Adhoc Departmental Moves" procedure outlined in section 5.
- **Digital project approval** (New Digital projects, new builds, major refurbishments, and upgrades/enhancements to existing systems) should follow the "Digital Project Approval" procedure outlined in section 6.

This procedure should be read in conjunction with the Health Board's Standing Financial Instructions, Standing Orders, the Policy for Procurement and Life Cycle Management of Equipment and where relevant, the Capital Investment Manual.

Templates and electronic links for the submission of projects are provided in the ICT Forms Library on the Health Board's Intranet site or through requests to the Informatics Service Desk.

Any project which may impinge on National Strategy may need to be submitted to the relevant Digital Health and Care Wales (DHCW) governance committees.

2. Objectives

The main objective of this procedure is to ensure employees of the Health Board are aware of the procedure to follow when requesting Digital equipment, software, services and new projects.

3. Scope

This procedure covers everyone that is employed by Hywel Dda University Health Board who may request Digital services.

4. Procurement of Standard Digital Equipment

This covers the purchase of all Digital standard hardware, software, peripherals (scanners, printers etc.) and mobile phones in addition to related professional services. This procedure does not include purchases which are part of an already approved capital programme, business case or DHCW funded projects.

Advice from Digital Services should also be sought where network attached equipment is being procured. This includes medical devices, laboratory analysers, security systems and CCTV.

All Digital equipment purchases will conform to Digital Services specifications and will be authorised prior to ordering by the Digital procurement team.

All Digital purchases should be channelled through Digital Services, if bypassed any Digital purchases should be clearly identifiable by Procurement who will forward such requisitions to the Head of Digital Operations to ensure that the processes in this procedure are followed.

Replacement Programme
When equipment is assessed as being “end of life” it will be replaced under the replacement programme subject to available funding levels. This will include but is not restricted to PCs, printers, scanners, servers, network devices, infrastructure components, software and telecommunications (including mobile phones).

The replacement programme is funded from the Health Board’s Discretionary Capital Programme (DCP) and will be managed by Digital Services. This does not exclude the funding of replacement equipment from departmental budgets (if less than £250) and Charitable Funds as required in line with the Health Board’s standing financial instructions.

New Equipment
The procurement of new Digital equipment will be from departmental budgets following approval and providing it doesn’t fall under the remit of the “New Digital Project” procedure requirements.

It is important to note that items over £250 in value and connected to the network are classed as capital assets (not revenue) and as such can only be funded from the Health Boards capital allocations and local charitable funds. This will include many pieces of Digital equipment including high end printers, PC’s, laptops and tablets.

All requests for software packages, computer hardware, peripherals (scanners, printers etc.) or network / telecommunication services should be made by completion of the request forms via the Digital Services Portal which is available under the “Request a service” link:

Welcome to the Digital Services Portal (opens in a new tab)

All sections in the form require completion for the procurement to progress and once received Digital Services will process in line with local procedures. The request must be authorised by the responsible officer (e.g. budget holder or service manager) and a notification will be received via Microsoft Teams to approve or deny the request.

Any request “deemed” as non-standard will be forwarded to the Head of Digital Operations for consideration and may fall under the remit of the “New Digital Project Approval” procedure as outlined in Section 8.

External Funding
Occasionally the Health Board will receive external funding which is placed into ring fenced budgets (Welsh Government R&D for example), requests utilising these monies will be managed as per this procedure and Digital Services will discuss with Finance on a case-by-case basis the funding arrangements and any revenue / capital transfers.

5. Procedure for Adhoc Departmental Moves

This section outlines the procedure that will be followed to gain approval for Digital to support departmental moves / changes and office moves. The scope includes Health Board employees requiring: -

- New data points for network access.
- New telephone points, handsets, and numbers.
- Moving of extension numbers between locations.
- Move of Digital equipment (PC's / Printers etc.) between locations.

It is important that Digital Services should be engaged as soon as possible using the process below to ensure any associated works can be scheduled in and completed prior to any staff moving offices.

All requests for departmental moves should be made by completion of the relevant electronic form on the Digital Services Portal. The link to the form is also provided below: -

Adhoc Network Moves and Changes : Hywel Dda University Health Board (wales.nhs.uk) (opens in a new tab)

All sections in the form require completion for Digital Services to process and once received the request will be completed in line with local procedures. The request must be authorised by the responsible officer (e.g., budget holder or service manager) and a notification will be received via Microsoft Teams to approve or deny the request.

On receiving the request Digital Services will review within 5 days and respond to the requester when the work can be completed and details of any associated costs. If the number of resources required by Digital is extensive then the "New Digital Project Approval" will be followed.

Once the budget holder has approved the work, Digital Services will complete a schedule for completion and any moves and changes requested which don't follow this procedure will be potentially rejected.

6. New Digital Project Approval Procedure

This section outlines the procedure that will be followed to gain approval and funding for a new Digital project which would be added to the Digital Operational Plan. Examples of such new projects include: -

- New builds or refurbishments of Health Board property which have a Digital element.
- Requests for upgrades to existing systems.
- Requests for new Digital system or service.
- Any requests received through the "Standard Digital Equipment Procedure" where the Head of Digital Operations determines it needs to follow the formal approval process.

Any such requests must be via the online request form available on the Digital Services Intranet Pages:

Digital Project / Support Request (opens in a new tab)

More information on the Health Boards Digital Response and framework can be found below:

Delivering the Digital Response (opens in a new tab)

The Digital project proposal once submitted will be discussed by the Digital Services Senior Management Team for consideration and prioritisation.

If approved by the Digital Senior Team and the project has already been funded and approved by the relevant assurance committee the project will be scheduled and have resources allocated.

If no funding / approval has been approved, then the request will be deferred to the Digital Programmes Group and Agile Digital Business Group as required for consideration.

7. Determining the Priorities for a Project

The following criteria will be used by the Digital Senior Team in assessing what priority should be given when approving projects: -

- The priority in this area / activity in the Health Board's IMTP.
- The project's time constraint.
- The potential savings that would be lost or additional cost incurred if the project was delayed.
- The resources required and any conflicts with other projects.
- Other projects / activities / initiatives dependent on the completion of this project.
- Any external influences on the project's implementation date.
- Risks incurred or changed by the implementation.
- The project's fit with national strategies if relevant.

8. Responsibilities

Head of Digital Operations
The Head of Digital Operations shall have overall responsibility for the implementation of this procedure and will delegate responsibility to ensure appropriate departmental procedures are in place to aid its implementation.

The Head of Digital Operations will escalate any issues as appropriate to the Digital Director.

Digital Senior Team
All members of the Digital Senior Team will be made aware of this procedure to ensure they are aware of their roles and responsibilities in the approval process for Digital projects.

NHS Wales Shared Services Partnership
The NHS Wales Shared Services Partnership will be required to be aware of this procedure to ensure any requisitions they receive for Digital related equipment is not processed unless this procedure has been followed (where requisitions are not received through designated Digital requestors).

Director of Estates
The Director of Estates will be responsible for dissemination of this procedure to relevant Estates staff to ensure it is considered when planning new builds and refurbishments of Health Board property.

Executive Directors / County Directors / Service Delivery Managers
Will be required to be aware of this procedure to ensure Digital implications are considered when planning service change, new projects, and new services.

Information Asset Owners
Information Asset Owners will be responsible for considering this procedure when planning any system upgrades or enhancements with 3rd party suppliers.

Heads of Department / Budget Holders
Will be required to be aware of this procedure to ensure it is followed when requesting Digital services.

9. Training

All staff will be made aware of this procedure through a communications plan and availability to view on the Health Board Intranet site.

Awareness will also be promoted by the Digital Service Desk when requests are received and through membership of the relevant governance groups of the Health Board.

Targeted communications will also be undertaken to the groups identified in the Responsibilities Section.

Support will be provided by Digital Services Department as required to support Health Board staff in ensuring they meet the requirements of this procedure.

Appendix A – Digital Requesting and Project Approval Flowchart