Information Security Policy

This document may be made available in alternative formats and other languages, on request, as is reasonably practicable to do so.

This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Policy Owner: ***Information Security Manager***

Approved by: ***Executive Team***

Issue Date: ***August 2016***

Review Date: ***August 2018***

Policy ID: ***HB50***

Changes made : 18.7 Do not attempt to access, or ask people to divulge information that you are not authorised to receive as part of your job; e.g. your own records, information relating to a family member or a friend.

INDEX

ABMUniversity HB

Version Control

Date of Revision	Summary of Changes	Date of Approval	Approved By	New Version No	Status
27/08/2009	Draft Policy			1.0	Draft
17/09/2009	Changes following IG group review 11/09/2009 / 18/09/2009			1.1	Draft
29/09/2009	Changes G Daly			1.2	Draft
8/10/09	Changes to Personal use of devices sect 13.8			1.3	Draft
26/10/09	Draft Policy as sent to Staff side for review – all changes accepted in doc			1.4	Draft
23/12/09	Policy Approved by Staff Side for presentation to Partnership forum			1.5	Final
4/2/10	Amended following review mtg with IP			1.6	Final
9/3/10	Policy Approved by Staff Side for presentation to Partnership forum			1.7	Final
August 2012	Annual review – No amendments			2.1	Final
September 2013	Annual review – Digit dictation machines added to examples of Removable media devices			2.2	Final
November 2015	Amendment agreed by IGC			2.3	Final

1. POLICY STATEMENT

Abertawe Bro Morgannwg University HB (the HB) holds and manages a great deal of information, much of it personal and confidential, without which it could not function. The purpose of information security is to enable information to be shared between those who need to use it while protecting information from unauthorised access and loss. The basic principles of information security should always apply:

1.1. Confidentiality:

The HB stores information that ranges from computerised records of patient registrations, hospital contacts and treatments through to paper based records with payroll details, personal files and patient case notes. The HB has a legal responsibility, which is shared by its staff to ensure that this data is not accessible to anyone without appropriate authorisation.

1.2. Integrity:

The HB has a duty to ensure that the data it holds is accurate, and remains accurate throughout the time it is held. This means that precautions must be taken to ensure that the data is not changed, through accidental misuse, deliberate abuse or even through the failure of a computer system to store it properly.

1.3. Accessibility:

Data is only useful if the people who need it have access to it. As a result, the HB must ensure that the people who depend on particular items of information, gain timely access.

2. SCOPE

2.1 This policy applies to all members of staff, students/trainees, secondees, volunteers and contracted third parties (including agency staff) of the HB, its hosted agencies and its managed units. This policy applies to all forms of information, including that stored on computers, transmitted across networks, printed on paper or other media, stored on tapes, disks, cameras or other electronic media, sent via e-mails and stored on databases. It applies to all information including paper records and the spoken word. It applies regardless of the location at which access to the information is gained. The aim of this policy is to ensure all staff are aware of and comply with, relevant legislation requirements and security standards.

2.2 Although the HB is not, at the time of this policy, targeted with meeting full compliance with ISO 17799/27001 it is an aim that the policy provides, as part of the annual review of the baseline, continual improvements towards that eventual goal. The standards are to be utilised for audit purposes as a set of good practices to be aspired to within the HB.

3. KEY RESPONSIBILITIES OF INFORMATION USERS

3.1 Comply with this policy and related policies, any local procedures and instructions.

3.2 Apply the basic principles of information security to all information, which they come into contact with.

3.3 Discuss any identified risks and security issues with line management or the Information Security Manager.

3.4 Report incidents by following the HB's incident reporting procedure.

3.5 All staff handling information (of any sort) within the organisation will have their responsibilities laid out in their job descriptions.

3.6 All staff are personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

3.7 Staff should operate a clear desk and clear screen policy. This means that any person, patient identifiable or organisationally sensitive information must be placed out of sight, in locked cabinets when not in use, and it should not be viewable on screen by anyone who does not have a legitimate need to see it.

3.8 Staff members that have been supplied with portable equipment for the purpose of home working (i.e. laptops or similar devices) are responsible for ensuring that it is regularly connected (i.e. at least every two weeks) to the HB network to ensure that upgrades for anti-virus software are installed.

3.9 As part of the employees terms and conditions of employment (contract) there will be an undertaking to maintain confidentiality of information. The duty of confidence will continue to apply after the contract of employment has ended.

3.10 Casual staff and third parties not covered by an employment contract will be required to sign a confidentiality agreement before being given access to information processing facilities.

4. KEY RESPONSIBILITIES OF THE HB'S MANAGEMENT

4.1 Ensure that all *information users* are provided with appropriate information security training.

4.2 Ensure that all *information users* comply with this policy and related policies, local procedures and instructions and ensure any changes are also communicated.

4.3 Ensure that *information users* have access to information that is appropriate to their role within the organisation.

4.4 Ensure that reported incidents are properly investigated and resolved.

4.5 Assess risks to information security and act to reduce those risks

5. PURPOSE

The policy aims to ensure that:

5.1 All systems are properly assessed for security

5.2 Confidentiality, integrity and availability of information are maintained

5.3 Staff are aware of their responsibilities

5.4 Procedures to detect and resolve security breaches are in place

6. ENFORCEMENT OF THE POLICY

6.1 The HB will conduct regular audits to monitor compliance with this policy. Failure to comply may result in disciplinary action or even prosecution.

7. LEGISLATION AND GUIDANCE

7.1 This policy will be brought to the attention of all new staff during the multi-disciplinary staff induction programme. At induction, the following legislation regarding the confidentiality of data is brought to the attention of new staff:

Caldicott Report
ISO27001 Information Security Standard
The Obscene Publications Act 1959 (amended)
Children Act 2004
The Police and Criminal Evidence Act 1984
The Business Regulations 2000, Interception of Communications Act 1985
The Criminal Justice Act 1988
The Copyright, Design and Patents Act 1988
The Computer Misuse Act 1990
Access to Records Act 1990
The EC Directive on Legal Protection of Databases 1996
The Human Rights Act 1998
Crime and Disorder Act 1998
The Public Disclosure Act 1998
Data Protection Act 1998
The Regulations of Investigatory Powers Act 2000
The Telecommunications (Lawful Business Practice (Interception of Communications Regulations 2000)
UK Terrorist Act 2000
Electronics Communication Act 2000
Freedom of Information Act 2000
The Health and Social Care Reform Act 2001
Privacy and Electronic Communications Regulations 2003

8. THE CALDICOTT REPORT – QUICK REFERENCE GUIDE

8.1 The Caldicott Committee was established to review the transfer of all patient identifiable information from NHS organisations to other NHS or non-NHS bodies for purposes other than direct patient care, or where there is a statutory requirement for information.

8.2 Caldicott Principles

The Caldicott Principles must be applied at all times in the management of patient identifiable data. The six Caldicott principles are:

1. **Justify the Purpose**
   Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

2. **Do not use patient identifiable information unless it is absolutely necessary**
   Patient-identifiable information should not be used unless there is no alternative.

3. **Use the minimum necessary patient-identifiable information**
   Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of anonymising the information as much as possible.

4. **Access to patient-identifiable information should be on a strict need to know basis**
   Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

5. **Everyone should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff are aware of their responsibilities and obligations to respect confidentiality.

6. **Understand and comply with the law**
   Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements

9. OTHER HB RELATED POLICIES AND PROCEDURES:

9.1 These policies should be read in conjunction with this policy and have sections that are relevant to this policy.

- E-mail Policy
- Internet Access Policy
- Records Management Strategy
- Minimum Retention and Destruction Policy
- Freedom of Information Act Policy
- Data Protection and Confidentiality Policy

10. TRAINING

10.1 All new staff must attend Multi Disciplinary Staff Induction where a session explaining the HB's Information Security Policy is presented.

10.2 Awareness sessions are scheduled regularly across the HB to inform staff of their responsibilities in relation to the confidentiality of data, Freedom of Information Act 2000, the Data Protection Act 1998 and good records management.

10.3 All staff should have appropriate training before being given access to systems.

10.4 Further information on HB IT training courses can be obtained from the IT Training Department or relevant system manager.

10.5 Line managers are responsible for ensuring that relevant policies are brought to their staffs attention during the local induction stage and new user authorisation process.

11. CONTROLLING ACCESS TO SYSTEMS

11.1 Access to computer services and to data will be controlled on the basis of business requirements, which take account of policies for information dissemination and entitlement.

11.2 System Managers will ensure that appropriate security controls and data validation processes, including audit trails, will be designed into application systems that store any information, especially personal or patient data.

11.2.1 STAFF

Access to all HB systems is controlled by user names and passwords. All new staff wishing to apply for a user name, all staff wishing to change their current access levels and all notifications of staff leaving must follow the relevant instructions on the HB's Intranet site.

11.2.2 3RD PARTY ACCESS

All 3rd party access can either be achieved via N3 with the relevant Statement of Compliance approval.

12. SECURITY AUDITS

12.1 The HB reserves the right to monitor use of any access to the HB's network. This encompasses all applications, network access and includes Internet access and email usage.

Reasons for monitoring include:

- Ensuring that the HB's policies and procedures are adhered to.
- Preventing or detecting unauthorised use or criminal activities.
- Maintaining the effective operation of the HB's communication systems.

12.2 Compliance with this policy will be monitored via a programme of security audits. Ad hoc audits may be undertaken by the Information Security Department at the request of Departmental Heads, Clinical Directors or other Senior Management.

13. COMPUTER SECURITY

To ensure the confidentiality and security of the data held electronically the following controls must be complied with at all times:

13.1 All PCs and Laptops will have a standard operating system and desktop.

13.2 Always log off or lock your computer (using Ctrl, Alt & Delete or Windows key & L) before leaving it unattended.

13.3 Do not allow unauthorised persons access to your computer.

13.4 Do not try to connect unauthorised devices to the HB's network e.g. modems, CD drives, iPods etc

13.5 Do not move your desktop computer without first contacting the IT Service Desk. All computers should be secured (via a steel cable to an anchor point) and security marked. Contact the IT Service Desk for further details.

13.6 Do not tamper with computer equipment or remove any components as this may invalidate the warranty, may endanger your safety and may be deemed as theft. All component changes are tracked using the HB's inventory management software and alerts are raised with the IT Service Desk.

13.7 All Computer equipment must be security marked and locked with a suitable security device. This does not apply to portable computer equipment; see Section 21 for security of portable computer equipment.

13.8 The utilisation of HB computers outside normal working hours for personal use is not permitted.

13.9 Use of HB computers by anyone other than the authorised staff member is strictly prohibited

14. ENERGY SAVING

14.1 Do log out and turn off all computer equipment (base unit and screen) at the end of the day and turn the power off at the wall socket where possible.

14.2 Do turn off printer and photocopying equipment as above.

15. STORAGE AND COPYRIGHT LAW

15.1 Only authorised freeware or shareware can be installed on HB computers. Do not install unauthorised or unlicensed software. It is a criminal offence to use illegal copies of software programs for which both the HB's Directors and individual employees may be liable if this policy is not complied with. Any employee illegally and knowingly reproducing software will be subject to the HB's disciplinary procedure.

15.2 All information and data stored on the HB's equipment is deemed to be HB property.

15.3 Copying or storage of anything that is not work related onto your computer is a breach of this policy.

15.4 Do not allow anyone to take unauthorised copies of software. HB owned software must not be taken home and loaded / installed onto an employee's home computer. If an employee has to use software at home for HB business, and is not provided with a HB computer for this purpose, a separate copy of the software must be purchased for the home computer.

15.5 All software, information and programs developed for and / or on behalf of the HB by employees during the course of their employment will remain the property of the HB. Duplication or sale of such software without the prior consent of the HB will be considered an infringement of the organisation's copyright and will be dealt with as a disciplinary matter.

15.6 Peer-to-peer sharing software, such as Kazza or WINMX, must not be installed onto any HB computers

15.7 HB computer equipment must not be used for any of the following activities:

The copying, saving or distribution of copyright media files e.g. MP3 or MPEG, games files, audio CDs or video DVDs

15.8 The playing of games files or illegally copied audio, video or digital music files e.g. MP3 / MP4.

15.9 No content that may be deemed as either illegal or offensive may be kept on any HB equipment.

15.10 Sending, receiving or storing of private photographs is prohibited.

16. CORRECT USE OF PASSWORDS

16.1 Do not try to log onto systems that you are not authorised to use.

16.2 Do not log in using another person's username and password.

16.3 Do not share your password.

16.4 Do not write your password down.

16.5 Do choose a password that is at least 8 characters including one non-alpha character.

16.6 Do not re-use passwords.

16.7 Do change your password immediately if you suspect that someone else knows it.

16.8 Do ensure that when entering your password, the entry cannot be seen by anyone else.

16.9 Where a user has forgotten his/her password and are unable to reset their Password using the system provided, they should contact either the relevant System Manager for clinical systems or the IT Service Desk where assistance will be given.

16.10 Do not store passwords in any program macro or function key.

16.11 Users will be forced to change their network password every 60 days. This helps protect the user from misuse of their account and protects the confidentiality of the information the HB holds.

17. GOOD PRACTICE WHEN CHOOSING A PASSWORD

17.1 All passwords should be 8 characters or more and should contain numeric as well as alphabetic characters e.g. m0rr1s0ns, where the ‘o‘s’ has been replaced by a zeros and ‘I’ has been replaced with a 1

17.2 If you have a problem remembering words, choose a line or two from a poem, song or phrase and use the first letter and then add in a number
e.g. **W**e **A**ll **L**ive **I**n **A** **Y**ellow **S**ubmarine and add **4**, the password would be **WALIAYS4**

17.3 Do not use this example, the name of your spouse, colleague, friend or pet, telephone number or car registration as these maybe too obvious.

18. INFORMATION GOVERNANCE

18.1 When dealing with all types of information please be aware of the requirements of the HB’s Record’s Management Strategy with regard to the retention and disposal of this information. This strategy can be found on the HB’s Intranet site.

18.2 When transporting or transferring data outside the HB be aware of the data protection and confidentiality policy and always check with the Information Governance Department or the Information Security Department who can provide guidance.

18.3 The distribution and storage of person identifiable information is governed by the Data Protection Act. To ensure that person identifiable information is dealt with correctly you must follow the guidance in the HB’s Data Protection and Confidentiality Policy, or if you have any queries contact the Information Governance Department.

18.4 Do not store confidential, person identifiable or business sensitive information on your computer’s local hard disk drive. Store it on a network drive where it will be secure and backed up on a daily basis. Saving data to the network aids sharing of this information where necessary.

18.5 All staff have a duty to ensure that information about patients is recorded accurately and in a timely manner. This is fundamental to patient care and the clinical and corporate governance of the HB. If patient information is found to be inaccurate on a system, it must be corrected either at source, or with assistance from the relevant system manager or the Information Department.

18.6 When exchanging person identifiable information with external agencies e.g. social services, ensure you comply with the relevant section in the Welsh Accord for the Sharing of Personal Information (WASPI). This protocol informs what information can be exchanged and what controls need to be put in place to ensure the safety of that information. Contact the Information Governance Department if you are unsure.

18.7 Do not attempt to access, or ask people to divulge information that you are not authorised to receive as part of your job; e.g. your own records, information relating to a family member or a friend.

.

18.8 Do not divulge information to those that are not authorised to receive it.

18.9 Do not leave confidential documents unattended, particularly on printers, photocopiers, fax machines or on desks.

18.10 Do not make unauthorised copies of confidential information.

18.11 The HB provides containers for the secure disposal of confidential and person identifiable information, ensure these facilities are used at all times.

18.12 The HB will make available, in a controlled manner, personal or patient information it holds in its offices required under statutory arrangements, to aid clinical and/or negligence investigations or to assist the Police if such information is required as part of a criminal investigation.

19. REMOVABLE MEDIA

19.1 Removable Media devices include USB 'sticks' (or memory sticks, memory 'pens', USB Flash Drives, etc), MP3 players, mobile phones/camera phones, cameras and Personal Digital Assistants (PDAs) such as Palm Pilot, iPAQ devices. Portable storage media also includes CDs, floppy disks, tapes, digital dictation machines etc.

19.2 Staff may not attach any personal removable media devices other than USB Memory Sticks to the HB network without prior permission of the HB Information Security Department.

19.3 Encrypted Removable Media must be used whenever Users need to process personal, patient identifiable or organisationally sensitive information away from the HB and then only if it is absolutely essential and in connection with their duties.

19.4 Removable media must not be left unattended except within secure official buildings.

19.5 Removable media must not be left in cars, even if secured out of view, or left unattended in public areas, e.g. public transport.

19.6 The user must be responsible for ensuring that no unauthorised person has access to the data held on the removable media both during and outside normal working hours - this includes access by family members if the removable media is used within the home.

19.7 It is not permissible to copy any PI Data to personal computers in the home.

19.8 Removable media such as memory sticks, floppy disks, CDROMs etc can be disposed of by contacting the IT Service Desk who will advise you on the correct procedures to be followed.

20. SECURITY INCIDENTS

20.1 Always report any incident using the agreed HB incident reporting procedure. Potential weaknesses in information security can be reported directly to the Information Security Department.

20.2 If you suspect your workstation has a virus or malicious software on it, report it immediately to the IT Service Desk.

20.3 In the case of accidental or unintentional access to inappropriate material (e.g. pornographic internet popup messages), inform the Information Security Department immediately (or as soon as possible for incidents occurring out of office hours), giving as much detail of the incident as possible. The incident can then be verified against the Internet security logs. Failure to report such incidents may result in disciplinary action.

20.4 Actual and suspected security breaches will, where necessary, be reported to appropriate bodies e.g. Police. Such incidents may result in disciplinary action and/or criminal proceedings being taken.

21. PORTABLE COMPUTERS AND HOME WORKING

21.1 The HB may at its discretion provide staff with portable computers for purposes of enabling them to work either within or outside their normal base of operations. Such members of staff will be expected to exercise all reasonable caution in their control and operation of said equipment, both at home, at other locations and in transit.

21.2 All staff members are responsible for the portable computer equipment in their care and as such must ensure that it is kept secure at all times. Place portable equipment out of sight whenever possible and preferably lock it away.

21.3 Staff members will be solely responsible for the security of both the equipment and information whilst stored within their home or off site.

21.4 Make sure that your laptop is properly secured, both in your office and whilst travelling. Be extremely cautious with laptops when using them on public transportation. Protect remote access procedure documentation, secure-id usernames and PIN numbers. Keep these items physically separate from the computer and carrying case.

21.5 Report loss or theft of laptops and portable equipment immediately to the police and relevant manager. It is the manager's responsibility to ensure that this is also reported through the HB's Incident Reporting Procedure.

21.6 The utilisation of HB ***portable*** computers outside normal working hours for personal use is not permitted. Use of HB portable computers by anyone other than the authorised staff member is also strictly prohibited.

21.7 Do not store confidential or personal identifiable information (PII) on portable computers unless it is encrypted. Contact the Information Security Department if your laptop is not encrypted.

21.8 If you are working on sensitive information be aware of the environment and ensure the screen or documents you are working on can not be seen by others. Working on sensitive or PI data in a public area should only take place when it is absolutely necessary.

21.9 Do not install software, regardless of its licence status, on HB portable computers. Any requirement for software should be discussed with the IT Department who will, if appropriate, facilitate its installation.

21.10 Ensure that information or programs no longer needed are effectively erased from all equipment and media. If you are unsure of how to do this contact the IT Service Desk for advice and guidance.

21.11 Do not save PII or confidential information to portable storage devices, e.g. Memory sticks unless they are encrypted. Contact the Information Security Department if you require help.

21.12 HB equipment must not be used to access the World Wide Web on home Internet connections unless achieved by using the HB approved connection software.

21.13 All security and monitoring software installed on portable computer equipment must not be disabled at any time.

21.14 Staff members that have been supplied with portable equipment for the purpose of working off site (i.e. laptops or similar devices) are responsible for ensuring that it is regularly connected (i.e. at least every two weeks) to the HB network to ensure that upgrades for anti-virus software are installed.

22. PHYSICAL SECURITY

22.1 Appropriate measures must be taken to protect all IM&T equipment against loss or damage and to avoid interruption to business activity.

22.2 Do ensure that local physical security procedures are followed. Security doors must be closed, properly locked and entry codes changed regularly.

22.3 Do not dispose of any equipment or media containing sensitive information. This should be carried out by a member of the IT Department, and with the knowledge of the relevant Systems Data Owner.

23. INTERNET USE

23.1 Guidance on the use of the Internet and the procedures to be followed for authorising Internet access can be found within the HB's Internet Access policy on the HB's Intranet site.

24. E-mail Use

24.1 Guidance on the use of the HB E-mail system and the procedures to be followed for authorising E-mail access can be found within the HB's E-mail policy on the HB's Intranet site.

25. STAFF LEAVING PROCEDURE

25.1 For further information on how to register staff terminations please refer to the instructions on the HB Intranet.

25.2 All managers must ensure they follow the HB procedures for staff leaving and ensure that all computer equipment e.g. Laptop, Secure-id token, memory sticks, door entry tokens are returned.

25.3 On receipt of a staff resignation line managers must discuss with the staff member which parts of their email account should be retained for business continuity purposes and share or forward any information required by the department to other staff members as directed. A user's e-mail account will be hidden for one calendar month after their last working day and will then either be deleted or if the account is on the 'CYMRU' domain then all access rights will be removed and the account disabled until the individual rejoins the NHS in Wales.

25.4 Managers are required to inform the IT Department of staff who are expected to be absent from the HB for a significant period of time e.g. on maternity leave or long term sick leave as these accounts can either be disabled until the user returns to work, an appropriate 'out of office' message can be set up or delegated access can be granted to another person within the department.

26. DISPOSAL OF COMPUTER EQUIPMENT

The following will apply to computers and other IT equipment identified as redundant or obsolete:

26.1 Any IT equipment identified as being redundant or obsolete by either the IT Department or the Department Manager can either be collected at a mutually convenient time or dropped off at IT Department.

26.2 Whenever possible, the IT Department will endeavour to reuse reconfigured and sanitised equipment for use elsewhere within the HB. Where this is not feasible the equipment will be securely disposed of in accordance with IT Department operational procedures.

26.3 The HB's IT asset register will be updated to reflect the status of the newly disposed equipment.

27. CONTROLS AGAINST MALICIOUS SOFTWARE MALICIOUS ACTIONS AND VIRUSES

27.1 The HB will seek to minimise the risks to software and information from viruses through education, good practice / procedures and by ensuring that the most up to date anti virus software is utilised on all PCs, Laptops and Servers.

27.2 The unauthorised configuration of anti-virus settings by anyone other than HB IM&T staff is prohibited.

27.3 All software installed must be appropriately licensed. The use of unauthorised software is prohibited. The maintenance of a register of software assets and licence compliance will be managed by the IT Department.

27.4 Users should report any detected or suspected computer viruses immediately to the HB IT Department.

28. DISPOSAL OF REMOVABLE MEDIA

28.1 For the purpose of this policy 'removable media' can be defined as any device that can be used to store electronic copies of data and which provides a removable, mobile medium for the transportation of this data. This includes but is not limited to the following CD and DVD, 3.5" floppy diskettes, high-density tapes, USB memory sticks and flash memory cards

28.2 Delivery must be in person and a receipt must be obtained from the IT Department. Use of the mail service is not appropriate for transporting removable media.

28.3 Removable media such as memory sticks, floppy disks, CDROMs etc can be disposed of by contacting the IT Service Desk who will advise you on the correct procedures to be followed.

28.4 Where the recycling of the removable media is an option, the IT Department will thoroughly erase any data that might reside on the media prior to reuse.

29. FURTHER INFORMATION AND CONTACT NUMBERS

29.1 A copy of this policy and other policies and procedures referenced in this statement are available on the HB's Intranet site. Contact details for the IT Service Desk, IT Training and Information Security staff can also be found on the Intranet site.

30. MONITORING AND AUDIT PROCEDURES

30.1 The Information Security Manager and the IT department will monitor compliance with this policy.

31. POLICY REVIEW

31.1 This policy is valid for 3 years but will be reviewed on an annual basis.

From: ABM Inquiries
Sent: 12 August 2016 15:16
To: Adel Davies (ABM ULHB - Community And Primary Care); Alexandra Howells (ABM ULHB - Execs); Amanda Hall (ABM ULHB - Executive Director); Amanda Smith (ABM ULHB - Postgraduate Centre); Angela Kind (ABM ULHB - Estates); Anne Biffin (ABM ULHB - Medical Directors Department); Bellina McNally (ABM ULHB - Women And Child Health); Beverley Edgar (ABM ULHB - Human Resources); Cathy Dowling (ABM ULHB - Corporate Nursing); Ceri Matthews (ABM ULHB - Clinical support services); Claire Birchall (ABM ULHB - Hospital Management); Darren Griffiths (ABM ULHB - Strategy); David Murphy (ABM ULHB - Health & Safety); David Roberts (ABM ULHB - Mental Health & Learning Disabilities); Debbie Bennion (ABM ULHB - Nursing Divison); Des Keighan (ABM ULHB - Estates); Dougie Russell (ABM ULHB - Musculo Skeletal); Eifion Williams (ABM ULHB - Finance); Eve Jeffery (ABM ULHB - Learning & Development); Fiona Reynolds (ABM ULHB - Singleton Hospital); Gemma Otter (ABM ULHB - Acct); Hamish Laing (ABM ULHB - Medical Directors Department); Helenna Jarvis-Jones (ABM ULHB - Musculo Skeletal); Hilary Dover (ABM ULHB - Primary and Community Services); Ian Phillips (ABM ULHB - Informatics Directorate); Jamie Marchant (ABM ULHB - Service Director); Jan Green (ABM ULHB - Interim DGM Surgical specialties); Jan Worthing (ABM ULHB - Singleton Hospital); Jonathan Goodfellow (ABM ULHB - Cardiology); Kim Clee (ABM ULHB - Workforce); Lesley Bevan (ABM ULHB - Nursing); Lesley Jenkins (ABM ULHB - NPT Locality); Linda Bevan (ABM ULHB - Surgical Specialties); Malcolm Thomas (ABM ULHB - Corporate Services); Martin Bevan (ABM ULHB - Neath Port Talbot Locality); Matthew Bunce (ABM ULHB - Finance); Mike Bond (ABM ULHB - Morriston Hospital); Mike James (ABM ULHB - Corporate Hospital Management); Nicola Williams (ABM ULHB - Morriston Unit); Paula Picton (ABM ULHB - Strategy); Rebecca Carlton (ABM ULHB - Corporate Hospital Management); Rhian Thomas (ABM ULHB - Estates); Robert Goodwin (ABM ULHB - Mental Health); Rory Farrelly (ABM ULHB - Nursing Divison); Sara Hayes (ABM ULHB - Execs); Sian Harrop-Griffiths (ABM ULHB - Strategy); Sian Passey (ABM ULHB - W&ch Nursing Women and Child Health); Silvana Gad (ABM ULHB - Primary & community Services Delivery Un); Steve Combe (ABM ULHB - Corporate Services); Susan Bailey (ABM ULHB - Communications); Susan Hunt (ABM ULHB - Bridgend Locality); Tersa Humphreys (ABM ULHB - Regional Services); Vanessa Bowkett (ABM ULHB - Learning Disabilities); Vicky Warner (ABM ULHB - Primary Care, Community Services); Victoria Gibbs (ABM ULHB - Trauma Orthopaedic & Spinal services); Wendy Penrhyn-Jones (ABM ULHB - Administration)
Cc: CatherineH Williams (ABM ULHB - CEO Office); Catrin Evans (ABM ULHB - Planning); Clare Dauncey (ABM ULHB - Human Resources); Diane Johnson (ABM ULHB - Finance); Francesca Devonald (ABM ULHB - Informatics Directorate); Gaynor O'Kane (ABM ULHB - Corporate Services); Linda Fifield (ABM ULHB - Corporate Services); Linda Smith (ABM ULHB - Nursing Divison); Lisa Harvey (ABM ULHB - Strategy); Lyn Westacott (ABM ULHB - Execs); Sian Millan (ABM ULHB - Executives)
Subject: Policies

I write to advise that the following policies have been updated and added to the Corporate Policies database:

- Data Protection & Confidentiality Policy
- Information Security Policy
- Media Handling Policy

The policies are available to view via the corporate policy database.

Llywodraethu Corfforaethol / Corporate Governance
Bwrdd Iechyd Prifysgol Abertawe Bro Morgannwg University Health Board
Pencadlys ABM / ABM Headquarters
1 Talbot Gateway, Baglan, Port Talbot, SA12 7BR
Bwrdd Iechyd Prifysgol ABM yw enw gweithredu Bwrdd Iechyd Lleol Prifysgol Abertawe Bro Morgannwg /
ABM Health Board is the operational name of Abertawe Bro Morgannwg University Local Health Board