CONFIDENTIALITY CODE OF CONDUCT
The Principals of Confidentiality for all staff

All employees working in/with 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 Data Protection Act 1998 and, in addition, for health and other professionals through their own professions Code(s) of Conduct.

This document outlines what confidentiality means for all of our staff giving detail to those who are already aware of this through their professional codes and outlining it in full to those staff who are covered under the Health Care support workers code of conduct. All staff working in the NHS in Wales have a responsibility to know about confidentiality. This documents purpose is to add more detail and inform staff of what this practically means in a day to day situation.

What does confidentiality mean?
Employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business “in confidence” information.

Cardiff and Vale University Health Board (the UHB) is committed to the delivery of the highest level of confidentiality for all the information that is holds. This means that we take every measure to make sure that all patient and staff information is processed fairly, lawfully and with as much transparency as possible so that the public and staff:

- Understand the reasons for processing personal information
- Give their consent for disclosure and use of their personal information
- Have confidence in the way the UHB handles its information
- Understand their rights to access information held about them

What is the principle behind this?
The principle is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the UHB’s security systems or controls in order to do so.

What does this document provide?
This document outlines your personal responsibilities concerning security and confidentiality of information relating to patients, staff and the organisation. This document has been produced to protect staff by making them aware of correct procedures so that they do not inadvertently breach any of the requirements placed upon them.

All employees of the UHB are expected to act and behave in accordance with the UHB values. It is essential that safety and respect in relation to any hospital related staff or patient information is maintained through the course of staff duties.

What information may be accessed
During your employment with the UHB you may acquire or have access to confidential information which you will have a legitimate reason to access and this is perfectly acceptable. However information that is accessed must not be disclosed to any other person unless it is required to be disclosed in pursuit of their/your duties or the individual concerned has given their specific permission or consent. This will apply during your relationship with the UHB and will also remain after you have left the organisation.

What are the different types of confidential information

- Patient records
- Staff records
- Recruitment and selection
- Telephone enquiries about patients /staff
- Electronic databases
- Methods of communication
- Use of fax machines
- Hand written notes containing patient information or staff information
- Video and sound files containing patient information or staff information

What is Personal Identifiable Information (PII)
Anything that contains the means to identify a living person. If there should be any doubt as to what information may be disclosed clarification must be sought from your line manager.

What are your responsibilities
Under the terms of your signed contract of employment you must, "at all times, be aware of the importance of maintaining confidentiality and security of information gained by you during the course of your duties. This will, in many cases, include access to personal information relating to service users. You must treat all information, whether corporate, staff or patient information, in a discreet and confidential manner in accordance with the provisions of the Data Protection Act 1998 and organisational policy".

- If unsure about the use or sharing of patient information, seek advice from your line manager, and line managers may need to seek advice from the organisation Caldicott Guardian who is the Medical Director.
- Breach of confidentiality may lead to disciplinary action and may be regarded as gross misconduct justifying summary dismissal

What does the Data Protection Act 1998 do
The Data Protection Act 1998 regulates the use of computerised information and paper records and images of identifiable individuals (patients and staff).

Data Protection Act and use of E-Mails
The use of emails is also covered by the act therefore caution should be taken when sending and forwarding emails within the UHB and extreme caution taken when sending emails outside of the UHB. Further details can be found on page 5 in the **Data Security and Information Technology (IT) section.**
The UHB is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

What must you be aware of with confidentiality
You must at all times be aware of the importance of maintaining confidentiality of information gained during the course of your duties. All information must be treated in a discreet and

confidential manner, and in accordance with the UHB's confidentiality principles, the Data Protection Act and the Data Protection and confidentiality policies which are available on the internet and intranet. Your duty of confidentiality arises out of the common law of confidentiality, professional and statutory obligations.

What would be considered as a Breach of Confidence

- Inappropriate use of health or staff records or abuse of computer systems may lead to disciplinary action, bring into question professional registration and possibly result in legal proceedings. All workers must therefore ensure that they are aware of the requirements and standard of required behaviour (see Confidentiality and Data Protection Act and your contract of employment details above).

What you can/cannot do

Your attention is drawn, in particular, to the following:

- Personal data protected under legislation must not be disclosed either verbally or in writing to unauthorised persons. It is particularly important that you ensure the authenticity of telephone enquiries.

- Written records, computer records and correspondence pertaining to any aspect of the UHB's activities must be kept securely at all times and be inaccessible to members of the public.

- Paper based person-identifiable information or confidential information requiring disposal should be done so in a confidential and secure manner where ever possible by the use of "Confidential Waste" bins.

- You must ensure that all computer systems that you use are protected from inappropriate access within your direct area of practice.

- If it is necessary to share information in order to effectively carry out your work, you must ensure that as far as is reasonable this information will be exchanged on a strictly 'need to know' basis, using the minimum that is required and be used only for the purpose for which the information was given.

- Conversations relating to confidential matters affecting patients/staff should not take place in situations where they may be overheard, e.g. in corridors, reception areas, lifts and cloakrooms. Given the highly confidential nature of the work you may undertake, you should understand that telephone conversations, in particular, should be conducted in a confidential manner.

- Any breach of the Confidentiality Code of Conduct and /or the IT Acceptable Use or Data Protection Policy may be regarded as misconduct and may be subject to disciplinary action, up to and including dismissal. Should you breach this clause after your employment has ended the organisation may take legal action against you.

- The same provisions apply if you are working off-site or at home.

- If you require an explanation concerning the interpretation or the relevance of this Code of Conduct you should seek advice from your line manager or the Caldicott Guardian.

- Any concerns regarding confidentiality issues within an area should be raised with the line manager in accordance with the relevant UHB policy eg Disciplinary/ Procedure for NHS Staff to Raise Concerns or with the appropriate individual if relating to the safety valve process.

- You will not at any time during your employment (except as so far as is necessary in the course of your employment) or afterwards, disclose to any person any information as to the business, dealings, practice, accounts, finances, trading, software, know-how, affairs of the UHB or any of the UHB's patients or prospective patients, distributors, firms or companies otherwise connected with the UHB. This does not affect your right to raise a concern if you think that something untoward is happening at work and wish to report this in a confidential manner (i.e. whistleblowing). Please refer to the Procedure for NHS Staff to Raise Concerns, a copy of which is available from your manager, on the UHB internet site or from the Workforce and Organisational Development function.

- Employees who are asked to access information relating to colleagues, friends or relatives need to declare their relationship to their line manager, who will decide if the task could be carried out by another staff member.

- All information held about the UHB or in connection with the UHB, and any of the above, is to be regarded as confidential. All notes, memoranda, records and other documents of the employer which may be in your possession are and shall remain the property of the employer and shall be handed over by you to the employer from time to time on demand and, in any event, upon termination of your employment.

- Any requests for information from the Media (newspapers, TV companies etc) should always be referred to the UHB Communication team. Requests for information under the Freedom of Information Act should be referred to the Information Governance Department or be handled via FOI email.

How does this affect Multi-Agency working

The UHB supports muti-agency working The principle requirement for such agencies is to ensure that they are not compromising anyone's trust or confidentiality. In particular, no agency should feel pressured to agree to a course of action which they consider is in conflict with their statutory obligations and wider responsibility, such as for public protection.

How can we share information within a Multi-Agency setting

If agencies are required to share information freely the appropriate documentation must be completed such as Information Sharing Protocol or a memorandum of understanding

What if people ask us to stop sharing/disclosing their information

Any individual can at any time make a decision to restrict or prevent disclosure or sharing of their personal information. Any such decisions must be respected by staff and noted within the patients records.

Data Security and Information Technology (IT)

- Staff should always log out of any computer system (by using the CTRL+ALT+ DEL buttons) or application when work is finished and must not leave terminals unattended and logged on.

- Personal passwords should be regarded as confidential and not be communicated to other individuals.
- Passwords should not be written down.
- Passwords should not be the employees own name or words or names associated with the individual (e.g. children's or pet's name or birthdays).
- Passwords should be alpha numeric and be a minimum of eight characters to comply with the IT acceptable use policy and Data Protection Policy

Transmission of Information

- The transmission of personal/patient identifiable information externally over the internet email (e.g. Hotmail, AOL, yahoo etc.) is prohibited.
- Personal /patient identifiable information should only be e-mailed to and from emails within the NHS network, i.e. addresses ending in @wales.nhs.uk.
- If regular e-mail is required to e-mails not within @wales.nhs.uk then alternative arrangements via secure file sharing portal can be arranged.
- Further information is available in the UHB IT Security Policy (Appendix 5 Internet/E-mail Policy).

Social media, mobile devices, non-UHB equipment

The use of patient identifiable information, including photographs via personal social networking sites is prohibited, as are staff details especially with regard to interactions in the work environment. Staff should refer to the UHB Social Media Guidelines see link below.
http://www.cardiffandvaleuhb.wales.nhs.uk/sitesplus/documents/1143/Social%20Media%20Guidelines%20rolled%20forward%20EPSG%2008%2004%2015.pdf and also the All Wales Social Media Policy see link below:
http://www.cardiffandvaleuhb.wales.nhs.uk/sitesplus/documents/1143/13.3.8%20All%20Wales%20NHS%20Wales%20Social%20Media%20Policy%20%20Final.pdf

- Removable devices such as USB Sticks, Portable Hard Disk drives or CD/DVDs must be encrypted.
- Personal and confidential UHB information may not be stored on any removable devices unless the device has been encrypted by the UHB.
- Information must not be stored permanently on mobile devices. If it is necessary to work away from the UHB, information should be transferred to the UHB server and deleted from the device as soon as possible.
- UHB confidential information must not be stored on non-UHB equipment, for example home personal computers, laptops, PDA's or SmartPhones. An exception is the synchronisation of your calendar, task list and address book with non – UHB PDA's which is permitted.

It is essential that before you use any of the UHB's IT systems you are familiar with and have completed the IT Security Policy including all associated appendices and also the UHB's Mobile Computing, Remote Access Policy available on the UHB's Intranet and from the UHB's Information Governance Department

Updating and Training

It is a mandatory requirement that all staff and others dealing with personal identifiable information keep up to date with IG training and developments.

Further sources of references you should refer to include:

Data Protection Act (1998)
Computer Misuse Act (1990),
Regulation of Investigatory Powers Act (2000)
Human Rights Act (2000).
Equality Act 2010
Confidentiality: Code of Practice for Health and Social Care in Wales
General Medical Council (GMC) Revised Guidance on Confidentiality
Nursing and Midwifery Council NMC Code of Conduct
Information Governance Policy
Data Protection Policy
IT Security Policy and all appendices
Social Media Guidelines
Personal Information Use and Disclosure of and the Duty to Share Guidance
Information Governance Review (To Share or not to Share)