CONFIDENTIALITY POLICY

<table>
<thead>
<tr>
<th>Author</th>
<th>Corporate Services Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Date</td>
<td>March 2001</td>
</tr>
<tr>
<td>This Revision</td>
<td>March 2005</td>
</tr>
<tr>
<td>Next Review Date</td>
<td>March 2008</td>
</tr>
<tr>
<td>Approved by</td>
<td>Management Board</td>
</tr>
<tr>
<td>Date of Approval</td>
<td>September 2005</td>
</tr>
<tr>
<td>Review Body</td>
<td>IM&amp;T Steering Group</td>
</tr>
<tr>
<td>Policy Number</td>
<td>01</td>
</tr>
<tr>
<td>Classification</td>
<td>Corporate Policy</td>
</tr>
</tbody>
</table>
Confidentiality Policy

1. Introduction

Confidentiality is a fundamental principle of the delivery of health services. Ceredigion and Mid Wales NHS Trust must preserve and maintain the confidentiality of the information we hold. Much of the confidential information held by the Trust is of a personal nature; the Trust holds information about patients, staff and volunteers. The Trust and its employees have an obligation not to disclose confidential information, be it personal or otherwise, as a result of various Acts of Parliament and NHS guidance. These are:

a. Data Protection Act 1998 – This Act was passed as a result of the EU Directive and it protects personal data held on all media. For more information, see the Trust’s Data Protection Policy.

b. Common Law Duty of Confidence – This is the duty placed on the Trust and other organisations as a result of case law regarding confidentiality.

c. Human Rights Act 1998 – This Act was passed as a result of the European Convention on Human Rights. This is intended to protect certain rights of individuals. In terms of confidentiality, the key part is Article 8 – “the right to respect for private and family life, home and correspondence”. This gives an individual the right to live their life with personal privacy in a way that does not infringe on the rights of anyone else. This could include information held about them in the form of diaries or personal records and the correspondence aspect is equally as broad.

d. Terms and conditions of employment – When any member of staff takes up a post with the Trust, their contract of employment includes certain terms and conditions. These include the requirement to maintain and protect the confidentiality of Trust information. All Trust staff are contractually required to adhere to this policy.

e. The Caldicott Committee Report on the Review of Patient Identifiable Information (1997) – This report investigated the transfer of patient identifiable information. The resulting management audit seeks to ensure that all NHS organisations protect the patient identifiable information that they hold.

f. Regulation of Investigatory Powers Act 2000 – This Act is intended to combat cybercrime. It ensures that any interceptions do not breach an individual’s human rights and requires that appropriate authorisations are obtained when required. The Act also supplements exiting legislation, for example any information collected under this Act still falls under the Data Protection Act and its principles.

g. Freedom of Information Act 2000 – This Act is part of the Government’s commitment to make more public sector information available to the public. It does, however, outline several exemptions to protect certain information. After 1 January 2005, these exemptions will form the basis of any decision to keep information confidential. (For more information see the Freedom of Information Act 2000 Policy).

h. Public Information Disclosure Act 1998 – This Act provides protection from victimisation and dismissal to members of staff who speak out against corruption and malpractice at work. Along with encouraging staff to disclose information in the interests of the wider public by offering employment protection, the purpose of this legislation is to recognise the contribution that public sector staff can make to delivering better services. For further information, see the Staff Concerns Policy.

i. Computer Misuse Act 1990 – This Act makes it a criminal offence to access or damage computer data without authority.
In addition to the above, health professionals will have ethical standards of confidentiality (e.g. NMC or BMA guidance). The duty of confidence continues after the death of the subject, the resolution or conclusion of the topic or the member of staff has left the Trust. The Trust is responsible for protecting all the information it holds, and information will be disposed of in accordance with the Records Management Policy.

No part of this policy is intended to counteract any statutory duty the Trust has to disclose information, such as the notification of infectious diseases.

2. **Scope**

This policy applies to:
- All employees of the Trust, including the Non-Executive Directors
- Volunteers
- Student/medical/work placements
- Agency/locum/bank staff
- All contractors and sub-contractors, and the Trust will ensure that all contracts will include a suitable confidentiality clause

In addition to the above, all official visitors to Trust premises must acknowledge the need to protect confidentiality.

3. **Definitions**

The Collins Dictionary (1988) defines something being confidential as:
- spoken or given in confidence, private
- entrusted with another’s secret affairs
- suggestive of intimacy

This brings a significant expectation from the individuals concerned. ‘Trust’ is central to the concept of confidentiality.

4. **Guidelines for practice**

Staff must not access any confidential information held in any form when they have no proper reason to do so in the course of their duties. When dealing with information of any nature, staff must be aware of their personal responsibility and undertake to abide by the policies and procedures of the Trust and their own departments.

4.1 **Personal information**

Personal information may relate to patients (both NHS and private), members of staff, visitors, carers, volunteers and other members of the public. To ensure the confidentiality of personal information, the following guidelines must be adhered to:
- Access to areas, departments or offices containing confidential information must be restricted to authorised personnel only.
- Recorded information of a personal nature must not be left unattended.
- Staff must not access any patient, employee or other record for which they have no proper reason to do so in the course of their duties within the Trust.
- Staff must not access records for their personal interest. This includes their own records.
• Staff in areas dealing with children, fertility treatments, abortion and GU medicine have additional constraints placed upon them.

4.2 Corporate information

Staff must ensure that corporate/business information is only viewed by those who need to see it in line with their role. Confidential information must not be left unattended unless in a secure environment.

4.3 Electronic records

All computer access must be password controlled. Passwords must be constructed to minimise the possibility of either being memorised by an onlooker or a guessed by a hacker or colleague. Staff must change their password at regular intervals or at any time they suspect that their password has become known. The IM&T Security Policy and the PC Security Policy provide more guidance on the formation and use of passwords. Staff must also log out of any computer system when leaving the machine unattended.

Managers must determine what systems staff have access to and the level of that access. The manager will ensure that their staff have the necessary training in the appropriate use of these systems.

4.4 Contracts

Staff contracts contain a statement enforcing the duty to respect the confidentiality of information.

Where contractors and employment agencies are used, the contracts between the Trust and these third parties must contain clauses to ensure that contract staff are bound by the same obligations as Trust staff.

Managers must ensure that staff are made aware of their responsibilities.

5. Removal or change of access

When a member of staff leaves or changes post within the Trust, their former manager must ensure that:

- Rights of access to computer systems are rescinded or changed to meet the needs of the employee’s new post
- Ownership of files and documents (held in any format) are transferred to another appropriate member of staff
- Identity badges are returned or changed to reflect the new post
- Any Trust property (e.g. keys) is returned
- The Department/Directorate Head will determine whether or not any digital door codes need to be changes (depending on the risks involved)

6. Storage

No document containing confidential information is to be left where it can be viewed by anyone without the authority or need to do so. This includes telephone messages, computer prints, faxes and other documents.
All hardware containing confidential data must be located in a secure environment. This applies to the major hospital systems, all file servers, personal computers, laptops and PDAs. (See the PC Security Policy and the Laptop and PDA Policy for more information).

7. Transport

Confidential information must always be transported in a manner that ensures that it is not accidentally disclosed to unauthorised individuals. Confidential information transported within the Trust must be in a sealed, addressed envelope (but not an internal mail/transit envelope). Personnel records should be hand delivered by the sending department or collected by the receiving department. Where this is not possible, the relevant departments must be told that information has been sent and confirm receipt.

Facsimile transmission must be sent in accordance with the Policy on the Secure Transmission of Manual Faxes. All faxes sent by any member of staff must have a front cover on – the Trust fax template is in the policy and must be used for both internal and external faxes.

Health records must be transported in accordance with the Policy for the Transportation of Case Notes.

8. Disclosure

Great care must be taken when discussing confidential information. Staff must ensure that they are talking to an appropriate person and that they are not easily overheard. If someone takes a call requesting personal information, they should ask the caller if they can return the call and take the name and number. Advice should then be sought from their line manager or the Data Protection Officer. For enquiries relating to staff, they can obtain advice as necessary from the Human Resources Department. This is especially important if the caller is trying to establish whether an individual is in the Trust (be it as a patient or member of staff).

8.1 Personal information (where the subject makes the request)

Under the Data Protection Act 1998, individuals have the right to receive copies of information held about them. Requests for this should be made in writing to the Data Protection Officer care of the IT Department. These will then be handled in accordance with the Subject Access Policy.

The Access to Medical Reports Act 1988 gives an individual the right (subject to certain exemptions) of access to any medical report relating to them which is to be, or has been, prepared by a health professional for employment or insurance purposes.

8.2 Personal information (by third parties)

Personal information can be disclosed:
- With the subject’s written, informed, explicit consent for a particular purpose.
- On a need to know basis if the person receiving the information is concerned with the treatment of a patient.
- If it is required by law or under a court order (If this is the case, the request should be referred to the Data Protection Lead).
- In child protection proceedings if it can be established that the information required is in the public interest.

In any situation, the Trust must be able to justify any decision to pass on information.
Personal information must not be disclosed under any circumstances for the purposes of fund-raising or commercial marketing.

The disclosure of information about HIV, AIDS, sexually transmitted diseases, assisted conception and abortion are restricted by law. This information must only be disclosed by one of a very limited number of authorised individuals and in accordance with the relevant legislation.

8.3 Telephone enquiries regarding staff

Wherever possible, enquiries about whether a member of staff is employed by the Trust must be passed to the Human Resources department. The department will take the details of the caller and the details of the individual they are looking for. Human Resources will then determine whether or not the individual works for the Trust and contact them to ask if there is any problem or issue with the caller. An appropriate response can then be passed to the caller.

The residential blocks should be treated as a private residence for telephone calls/enquiries. This means that if the caller does not have the direct number or extension they wish to be connected to, they should not be transferred directly. Switchboard should ask for the identity of the caller, put them on hold and speak to the member of staff concerned to determine if they are prepared to take a call from that person.

There is also a need for staff to inform the switchboard and Human Resources department if they are receiving and/or trying to prevent nuisance calls, giving as much information as possible. This will enable them to filter calls appropriately. The Trust will endeavour to ensure that nuisance or malicious calls are blocked, but cannot guarantee that all calls will be blocked.

8.4 Children and young people

People aged 16 and over are regarded as adults and must be asked for consent to disclose information. People under 16 who have sufficient understanding and intelligence can also give consent (Fraser competence), otherwise the parent or guardian must be asked for consent.

In child protection cases the interests of the child must be safeguarded. A child or young person up to the age of 18 may need protection from an inter-agency child protection plan. It may be necessary to pass on information without the consent of the parent or guardian. In these cases, the request must be referred to the child protection nurse and the consultant most recently responsible for the child’s care.

8.5 Corporate information

Corporate/business information may only be disclosed or released in line with the appropriate day-to-day conduct of Trust business. On other occasions, the request must be made in writing to the Head of Corporate Services. From 1 January 2005 requests will be dealt with in accordance with the Freedom of Information Act 2000 (see the Freedom of Information Act 2000 Policy).

8.6 Disclosure to the media

Requests for information from the media in relation to a serious incident must be dealt with in accordance with the Media Policy. Requests for information regarding the condition of a patient should be referred to the Duty Manager. Other requests for information from the media must be referred to the Head of Corporate Services or the Duty Manager.
8.7 Litigation

Requests for information in relation to litigation must be dealt with by the Complaints and Litigation Officer in conjunction with the Head of Corporate Services and the Data Protection Officer.

8.8 Police enquiries

In the course of their inquiries, the police may wish to obtain personal details regarding an individual that relates to an alleged offence. The police have no automatic right to such information without providing the individual’s explicit, informed consent to disclosure in writing. It may not always be possible to seek consent as it may impede the police inquiries or warn off the suspect. In this situation, requests must be referred to the Duty Manager who will consider (with reference to the Police Access to Personal Information Procedure – needs to be written) whether the request can be granted. On occasions where the Duty Manager required further clarification on Data Protection issues or requires a second opinion from an Executive when refusing information, they can contact the Data Protection Lead or the Executive on call as appropriate.

9. Disposal

Records will be disposed of in accordance with the Trust’s Records Management Policy.

10. Training

Training on confidentiality, Data Protection, Freedom of Information and IT Security will be included in the Trust’s training and development plan. All new members of staff are required to attend induction training, which will include these areas. This training will also be included in the Trust’s mandatory training programme, which existing members of staff are required to attend.

It is essential for the principle of confidentiality to become embedded in all development activity

11. Advice and assistance

If any member of staff has any queries regarding personal information, they should contact the Data Protection Officer. If the query is regarding corporate/business information, they should refer to the Head of Corporate Services. Both will consult appropriately with colleagues and provide advice.

12. Breaches of confidentiality

Staff are contractually obliged to abide by this policy. Any breach of confidentiality must be reported to the Head of Corporate Services and to the line manager concerned.

Any breach of this policy will be dealt with in accordance with the Trust’s Disciplinary Policy.

13. Review

This policy will be reviewed in March 2008. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation.

---