Chelsea and Westminster Hospital NHS
NHS Foundation Trust

CONFIDENTIALITY CODE OF CONDUCT FOR STAFF

Chelsea and Westminster Hospital NHS Foundation Trust is committed to the delivery of a first class confidential service. This means ensuring that all patient and staff information is processed fairly, lawfully and as transparently as possible so that the public and staff:

- understand the reasons for processing personal information
- give their consent for the disclosure and use of their personal information
- gain trust in the way that the Trust handles information, and
- understand their rights to access information held about them.

This Code of Conduct outlines your personal responsibility concerning security and confidentiality of information relating to patients, staff and the organisation.

All employees of the Trust are expected to act and behave in accordance with the Trust values of safety and respect in relation to any hospital related staff or patient information that they may encounter during the course of their duties.

During the course of your time within the Trust, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the Trust. This condition applies during your relationship with the Trust and after the relationship ceases.

Confidential information includes all information relating to the Trust and its patients and staff. Such information may relate to patient, staff records, recruitment and selection, telephone enquiries about patients or staff, electronic databases or methods of communication, use of fax machines, hand-written notes made containing patient information etc. Personal identifiable information is anything that contains the means to identify a person. If you are in doubt as to what information may be disclosed, you should seek clarification, and if appropriate prior permission, from your line manager.

The Data Protection Act 1998 regulates the use of computerised information and paper records and images of identifiable individuals (patients and staff). The use of emails is also covered by the act ***therefore caution should be taken in sending and forwarding emails within the Trust and extreme caution taken in sending emails outside of the Trust***. The Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

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 Trust's Confidentiality Code of Conduct, the Data Protection Act, The Trust's IT Acceptable Use and Data Protection and confidentiality Policies available on the Trust intranet.

Your duty of confidentiality arises out of the common law of confidentiality, professional and statutory obligations, the NHS Code of Practice on Confidentiality

and your contract of employment or engagement. Breaches 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).

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

- Data protected information 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 Trust's activities must be kept securely at all times and inaccessible to members of the public. Paper based person-identifiable information or confidential information requiring disposal should be done so in "Confidential Waste" bins, located throughout hospital premises.

- 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 and Confidentiality 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 Trust's Caldicott Guardian. Any concerns regarding confidentiality issues within an area should be raised with the line manager in accordance with the relevant Trust policy eg Disciplinary/ Whistleblowing Policies.

- 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 Trust or any of the Trust's patients or prospective patients, distributors, firms or companies otherwise connected with the Trust. 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 Trust or in connection with the Trust and any of the above is to be regarded as confidential. All notes, memoranda, records and other documents of the employer and 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 Trusts Communication team. Requests for information under the Freedom of Information Act should be referred to the IMT Directorate or be handled via FOI email.

Data Security and Information Technology (IT)

Staff should always log out of any computer system (by using the CTRL+ALT+ DEL buttons or the Windows logo plus L) or application when work is finished and 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 to comply with the IT acceptable use policy and Data Protection and Confidentiality Policy and DH guidance.

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 nhs-net accounts if doing so externally or internally through the chelwest email system.

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 Trust's Social Networking websites Policy.

It is mandatory that all Removable Devices such as USB Keys, Portable Hard Disk drives or CD – Rom's are encrypted. The Trust has implemented Checkpoint PointSec Endpoint Security which has a centrally managed policy which enforces that all such devices to be encrypted prior to use.

Personal & Confidential Trust information may not be stored on any Removable Devices unless the device has been encrypted by the Trust.

We discourage the use of personal USB keys and would advise that you use only Trust purchased devices. The uses of camera phones for the transmission of personal/patient identifiable information are also prohibited. Confidential Trust information may only be stored on mobile devices with the permission of your line manager or the Trust's Information Security Manager/Caldicott Guardian.

Information must not be stored permanently on mobile devices. If it is necessary to work away from the Trust, information should be transferred to the Trust server and deleted from the device as soon as possible.

Trust information must not be stored on non-Trust 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 – Trust PDA's which is permitted.

It is essential that before you use any of the Trust's IT systems you are familiar with and have completed the IT Acceptable User Policy and also the Trust's Mobile Computing, Remote Access and Telecommunications Policy both of which are available on the Trust's Intranet and from the Trust's IM&T 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 and to undertake annual Information Governance exercises e.g. completing questionnaires to confirm that they have done so.

Further sources of references you should refer to include:

DOH guidance: Confidentiality, NHS Code of Practice
DOH guidance: Confidentiality, NHS Code of Practice: Supplementary Guidance: Public Interest Disclosures.
Professional Codes of conduct e.g. AHP, GMC,NMC, Managers and Pharms,

Trust Policies
Data Protection and Confidentiality Policies
Use of Social Networking Websites policy
Web Communications Policy
Media Policy
Whistleblowing Policy
Disciplinary Policy

This code applies to all staff, including temporary, honorary, agency, contracted workers, volunteers, students and work experience/observers.

DECLARATION

I, have read the Trust Confidentiality Code of Conduct. I understand, by signing this declaration, that I will comply with its requirements and should I breach this code, I may face disciplinary action and possibly dismissal.

Signed: .....

Employee Name in Capital Letters: .....

Department: .....Date: .....

CONFIDENTIALITY CODE OF CONDUCT FOR STAFF	
Formally ratified at the Trust Joint Management and Trade Union Committee **Minor text changes approved by Information Governance and Consultative Commitees**	**Date**: 12th February 2009 Date: 14th February, 2013
COMMITTEE APPROVAL:	**CHAIR'S SIGNATURE:** **STAFF SIDE SIGNITURE:**
Date of next review: **February 2013**	

Signed copy to be returned to Human Resources, Unit 111, Harbour Yard, to place on personal file