York Teaching Hospital NHS

NHS Foundation Trust

Code of Conduct for Employees in Respect of Confidentiality

Code Prepared by: Manni Imiavan Head of Information/Data Protection Officer	Code Approved by: Information Governance Steering Group	Date Next Review Due:	01/03/2013	
Date Prepared: 01/03/2011	Date Approved: 08/03/2011	Date Review Takes Place:	01/03/2013	

Please note that this document should normally be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear please contact your manager.

1. Purpose of Code

This code sets out the standards expected of staff in maintaining the confidentiality of patient information.

2. Legal Framework Governing Confidentiality and Staff Responsibility

All staff have a personal duty of confidence to patients and to the Trust.

The duty of confidence is conferred by common law, statute, for example the Data Protection Act 1998, contract of employment, and where applicable, professional registration.

3. What is Considered Confidential Information?

Personal information is data from which a living individual could be identified; this may include information such as name, age, address, and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.

Information is confidential when it is personal information given to someone who has a duty of confidence (the Trust staff) in the expectation that it will not be disclosed without the consent of the provider of the information.

Personal information may be known or stored on any medium. Photographs, videos, etc are subject to the same requirements as information stored in health records, on a computer, or given verbally.

4. Keeping it Confidential: Following Trust Policies and Procedures

The following policies and procedures have been put in place to support the confidential handling of information and should be followed by all staff:

- **Data Protection and Confidentiality Policy** (sets out the policy and procedures around the secure transfer of data, collecting consent and maintaining confidentiality within the Trust);
- **Safe Haven Policy** (sets out the policy and procedures on the protection and secure handling and transmitting of person identifiable or sensitive information);

- **Incident Management Policy** (sets out the policy and procedures for responding to a security breach);
- **Business Continuity Policy** (sets out the policy and procedures in the event of systems failure);
- **Removable Media Procedure** (provides guidance for staff that use portable devices and removable media);
- **Access Control and Password Management SOP** (sets out procedures for the management of access rights to computer-based information systems).

All staff need to ensure they are aware of the procedures that are relevant to their role and comply with them.

5. Passwords, smartcards and security

All users will be assigned a level of access to PAS and other system that is appropriate to their role. Personal passwords should be regarded as confidential and those passwords must not be communicated to anyone or written down.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to your line manager.

6. Use of Email and Web-based Services

Email and internet usage should be restricted to work related issues.

7. Circumstances where Confidential Information can be disclosed

The Trust will inform service users, staff and any other data subject why, how and for what purpose personal information is collected, recorded and processed. This will be achieved by leaflets and information provided face to face in the course of a consultation.

Personal information may be disclosed with patient consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality. Consent may be implied or explicit.

Explicit consent of the data subject is required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

Explicit consent may be given in writing or verbally. A basic explanation of what information is to be disclosed and why / what further uses may be made of it, must be provided to the data subject together with a description of the benefits that may result from the proposed sharing of information and any risks if consent is withheld.

Personal information may be disclosed without consent in certain circumstances, for example:

- Where permitted by law, for example where public interest overrides the need to keep the information confidential.
- Where the Trust has made a decision based on the key factors of necessity and proportionality;

All requests for disclosure without the consent of the data subject, including requests from the police, should be referred to the Trust Information Governance lead.

8. Dealing with Subject Access issues

Subject Access requests should be dealt with by the Trust's IG Lead. Patients are charged a fee of £10 for Subject Access Requests. The requested information must be provided within 40 days. The patient should be asked to provide their name, address, postcode and date of birth to ensure correct identification of the patient's records. The patient request should be in writing. The patient should be asked to provide identification before the records are shared, for example their passport, full driving license, a credit card etc. The patient should be asked to either collect the information in person from the Trust or consent to the record being posted to them.

9. Offsite/Home Working Arrangements

Patient identifiable information must not be removed from the Trust.

However, patient identifiable information may be used outside of the Trust in certain circumstances, for example as part of contracted job, at an inquest, legal proceedings, or the delivery of effective healthcare within the community.

Explicit authorisation must be obtained from the Trust's Caldicott Guardian if patient identifiable information is required to be removed from the Trust.

10. Support

For assistance with disclosure issues, please contact the Information Governance lead.

11. Abuse of Privilege and Breach of confidentiality

It is strictly forbidden for employees to look at information about any patient including any information relating to their own family, friends and acquaintances unless they are directly involved in the patient's care or with administration on behalf of the Trust. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

12. Possible Sanctions for breach of confidentiality

Breach of this code could lead to disciplinary action. Depending on the circumstances this could range from remedial training to dismissal. Prosecution or an action for civil damages may also be taken under the Data Protection Act 1998.

13. Trust Information Governance: Key Personnel

- **Senior Information Risk Owner (SIRO):** Head of Finance and Procurement
- **Caldicott Guardian:** Deputy CEO/Director of Nursing
- **Confidentiality Officer:** Head of Corporate Governance
- **Data Protection Officer/ IG Lead:** Head of Information

- **Information Security Officer:** Head of IM&T

14. Staff Declaration

TO BE COMPLETED BY THE EMPLOYEE

I understand that I am bound by a duty of confidentiality and agree to adhere to this Code of Conduct and the requirements of the Data Protection Act 1998.

EMPLOYEE NAME:

SIGNATURE: **DATE:**

SIGNED ON BEHALF OF YORK TEACHING HOSPITAL

MANAGER'S NAME: AMY MESSENGER

SIGNATURE: AMessenger **DATE:**

POSITION: NURSE BANK MANAGER