Wrightington, Wigan and Leigh NHS Foundation Trust

Staff Confidentiality Code of Conduct

your hospitals, your health, our priority

CONTENTS: **PAGE No:**

Introduction **2**
2

1. **Code of Conduct Statement** **2**
2. **Key Principles** **3**
3. **Responsibilities** **4**
4. **What is confidential patient information?** **5**
5. **Data Quality and Record Keeping** **5**
6. **Freedom of Information** **6**
7. **Information Sharing** **7**
8. **Protecting and Securing information** **9**
9. **Transportation of information** **9**
10. **Requests for personal information** **9**
11. **Retention and Disposal of information** **11**
12. **Incident Reporting** **11**
13. **Training and Improving Knowledge** **12**
14. **Social Networking / Media** **12**
15. **Auditing** **12**
16. **Non compliance** **12**
17. **Whistle Blowing (Open Door Policy for Handling Staff Concerns)** **12**

Appendices

1. **References and further information** **14**
2. **Confidentiality Code of Conduct Disclaimer** **15**
3. **Glossary of Terms** **16**

AT ALL TIMES STAFF MUST TREAT EVERY INDIVIDUAL WITH RESPECT AND UPHOLD THEIR RIGHT TO PRIVACY AND DIGNITY

INTRODUCTION

The Confidentiality Code of Conduct is based on the Department of Health's Code of Practice "Confidentiality: NHS Code of Practice"; legislation such as the Data Protection Act 1998, the Freedom of Information Act 2000 and the Computer Misuse Act 1990 and other Department of Health Information Governance guidance such as Records Management: NHS Code of Practice. This code of conduct sets out working practices to effectively deliver information governance standards that are required by the law, ethics and policy.

1. STATEMENT

1.1 The Trust is committed to enabling those working with information to have an effective understanding of their obligations regarding confidentiality and information security. This document describes those responsibilities and provides guidelines in order to ensure that confidentiality and information security is maintained.

1.2 The Confidentiality Code of Conduct applies to all established and temporary employees, non-executive Directors, governors, volunteers, students and all individuals who work under a contract for services with the Trust. For the purpose of this policy hereafter these groups will be referred to as `staff`. The Confidentiality Code of Conduct applies whilst these persons are on site and off site as the duty of confidentiality applies even where an individual is no longer representing the Trust.

2. KEY PRINCIPLES

2.1 The key principle of the Confidentialty Code of Conduct is that no staff shall breach their duty of confidentiality, allow others to do so or attempt to defeat any of the Trust's information security systems in order to do so.

2.2 The Trust has a legal duty to service users and staff (and others who are in contact with the Trust) to:

1. Protect their personal information
2. Inform them how that information is being/will be/has been used
3. Inform them of their rights to access personal information

2.3 It must be remembered that whilst ordinarily the Trust's policy is to seek consent prior to disclosure of personal information, in certain circumstances the Trust may disclose the information without consent. See the Use, Consent and Disclosure of Information Policy for further information.

2.4 This document outlines the duty of confidentiality and the Trust's expectations in respect of data processing. Data Processing is anything that the Trust does with data whether this be using, sharing, editing, deleting, transporting (the list is exhaustive). This policy is designed to ensure that the Trust operates in such a way as to safeguard the confidentiality of patient and staff information. It assists them to have confidence in the way we work and deal with personal and / or sensitive data.

2.5 This document :

1. Introduces the concept of confidentiality
2. Provides a summary of the main legal requirements in respect of confidentiality including the Data Protection Act 1998, the Access to Health Records Act 1990, Computer Misuse Act 1990 and the guidance contained within the Caldicott Principles 2013
3. Provides practical guidance for addressing common problems regarding personal data
4. Provides guidance regarding information sharing
5. Provides information about the Information Commissioners Office and monetary penalties

3. RESPONSIBILITIES

3.1 Responsibility of the Trust Board

3.1.1 The responsibility for the provision of a Confidentiality Code of Conduct rests initially with the Trust Board.

3.1.2 The Trust Board will ensure, through the line management structure, that this code is applied fairly and equitably and that all relevant persons are aware of the standards of conduct required.

3.2 Responsibility of the Information Governance Department & Human Resources Directorate

3.2.1 The Human Resources Directorate and the Information Governance Department will oversee the introduction; operation and monitoring of this code of conduct and will report to the Trust Board on a regular basis to ensure the fair and consistent application of the code throughout the Trust.

3.3 Responsibility of the Caldicott Guardian

3.3.1 The Caldicott Guardian will oversee the disclosure of individual personal information with particular attention being paid to extraordinary disclosures (those which are not routine) in accordance with the Confidentiality: NHS Code of Practice and the Caldicott Guardian Manual .

3.4 Responsibility of the Senior Information Risk Owner (SIRO)

3.4.1 The SIRO who is the Director of Finance and IM&T is responsible for:

1. Ensuring that an overall culture exists that values and protects information with the organisation
2. Owns the organisations overall information risk programme and risk assessment process, tests its outcome and ensures that it is used
3. Advising the Chief Executive on the information risk assessment process, test its outcome and ensure that it is used
4. Advising the Chief Executive on the information risk aspect of their statement of internal control.
5. Owning the Trust's information incident management framework

3.5 Responsibility of Managers

3.5.1 Line Managers are responsible for ensuring that staff are aware and understand the Confidentiality Code of Conduct.

3.6 Responsibility of Employees

3.6.1 Staff are responsible for adhering to the Confidentiality Code of Conduct and ensuring they understand the content. If they do not they should raise this with their Line Manager.

3.6.2 Staff are responsible for agreeing to the confidentiality disclaimer on commencement of employment

3.6.3 Failure to maintain confidentiality in accordance with this code could lead to disciplinary proceedings being brought.

4. WHAT IS CONFIDENTIAL PATIENT INFORMATION?

4.1 A duty of confidence arises when one person shares information with another in circumstances where it is reasonable to expect that the information will be held in confidence. An example of this would be in a patient to doctor consultation. The Department of Health's guidance: Confidentiality: NHS Code of Practice, states that the code of practice has 3 core aims:

1. To protect patient information
2. To inform patients effectively about the uses to which their personal information will be put, with no surprises
3. To provide choice to patients as far as possible about the use of their personal information. In some circumstances, where this is required by law for instance, under the provisions of section 251 of the NHS Act 2006, information may be used without patients being informed

4.2 Maintaining confidence is:

1. A legal requirement which is underpinned by case law
2. A requirement of professional codes of conduct within healthcare
3. A specific requirement of the contract of employment within the Trust and is linked with disciplinary procedures

4.3 Patients entrust the Trust with the most sensitive of personal information that relates to their health and other matters as they seek treatment. Not only do they give the Trust this information, they also allow the Trust to gather this information from other sources. They do this because they have confidence in the Trust to treat this information in an appropriate manner. Principle 1 of the Data Protection Act principles states that information must be processed fairly and lawfully. The public have a legitimate expectation that all staff will respect their privacy and act appropriately. On occasions, the patient cannot directly express this willingness to entrust us with their sensitive personal information, because they lack capacity, this in no way diminishes our responsibilities to them.

4.4 Information which identifies an individual must generally only be used for the provision of the healthcare of that individual. If it is to be disclosed or used for any other purpose, it is necessary to satisfy one of the following criteria:

1. The patient's consent to the disclosure has been obtained
2. There is a positive legal duty to use or disclose the information

3. There is a significant risk to others if the information is not used or disclosed.
4. Disclosure is in the wider public interests and can be justified by reference to relevant statutes

4.5 Unless there is a valid reason for using information that identifies a patient, then anonymised information should be used.

4.6 Further information regarding the above can be found in the Use, Consent and Disclosure of Information Policy.

5. DATA QUALITY & RECORD KEEPING

5.1 Information must be adequate, relevant and not excessive (principle 3 of the Data Protection Act 1998) and it must be accurate and up to date (principle 4 of the Data Protection Act 1998). All staff in the organisation have a responsibility to ensure patient demographic information is validated at each face to face visit and all data relating to patient activity and clinical details are captured contemporaneously in both paper and electronic format where relevant.

5.2 Staff must also ensure that any corporate information is accurate, reliable and up to date (for example, polices and procedures, minutes of meetings, financial information) in order to comply with the above Data Protection Act principles, the Freedom of Information Act 2000 and the Records Management: NHS Code of Practice. For further information, please read the Freedom of Information Procedure and the Corporate Records Management Policy and Procedure.

6. FREEDOM OF INFORMATION

6.1 The Freedom of Information Act (FoI), gives the general public a right of access to all types of information recorded by public authorities. The Trust has a legal obligation to comply with the Act. Failure to do so is a criminal offence. The Trusts compliance with the Act will be monitored by the Information Commissioner's Office (ICO).

6.2 The Act supplements and complements the DPA 1998, which gives individuals the right to access personal information about them held by the Trust. The Act gives access to all other forms of information which is held by the Trust and it therefore has a more extensive scope than the DPA. These two Acts together will enable the public to access most records held by the Trust.

6.3 You must be aware that potentially any piece of information that has been recorded by staff could be made available to the general public on request.

6.4 You must also ensure that if you are asked to provide information in order to answer a Freedom of Information request this must be responded to within the timescale set with the information provided or with reasons why the information cannot be provided. If you are not the correct person to be dealing with a particular question(s) for a Freedom of Information request, you must inform the Information Governance Service as soon as possible.

7. INFORMATION SHARING

7.1 Principle 2 states that personal information must be process for limited purposes. However, there are many occasions when information needs to be shared with other service providers and individuals not directly associated with a patient's own care, such as

clinical auditors. It is imperative that patients are aware that in certain circumstances their personal information must be shared. A patient would probably expect information to be shared with other service providers, but would not, perhaps, expect clinical governance or clinical audit teams to be privy to their records.

7.2 It is important that the patient is informed of the full extent of information sharing, this is undertaken via the "How we use your Personal Information" leaflet available on the Trust website. It is particularly important that patients are aware that, on some occasions, information is released to non-NHS bodies.

7.3 There is also the need for confidential information to be shared with individuals that do not contribute to or support a patient's healthcare treatment. Although the patient may not consider these areas important, they underpin the functioning of the NHS and contribute to the society in which we live. Examples of these are medical research, health service management and financial audit. It should not be assumed that patients who seek healthcare are content for this information to be used in this way and steps must be taken (as set out in paragraph 5.2) to ensure that they understand this and have an opportunity to object. In some cases, the Trust can use data if this has approval under Section 251 of the NHS Act 2006.

7.4 Patient Consent to Disclosing - The ideal would be to obtain the patient's consent to each occasion of sharing of identifiable information. However, it is recognised that this is not always practicable. The recommendation from the Information Commissioner and the Department of Health is that where information is shared for healthcare purposes, then the patient's implied consent is sufficient. This means that the patient does not need to give explicit consent to the sharing of their information on each occasion. Instead patients must be notified of the uses to which their information may be put and their continuing presence to receive care implies that they have given consent to the sharing of their information in order to provide that care, for example, patients must be informed about text messaging

7.5 At the same time, patients, generally, have the right to object to the sharing of confidential information that identifies them. In all cases, they should be made aware of this right to object. However, if they wish to exercise this right it may mean that they cannot be given the full care that would be of benefit to them. In some exceptional cases, they may not be able to be cared for at all. Doctors and other members of the clinical team may not be able to treat a patient safely unless they have full access to all relevant information, including a patient's condition and their medical history. For more information about information sharing with other organisations, please contact the Information Governance Service.

7.6 The NHS Care Records Guarantee, issued by the Department of Health in May 2005, acknowledges the discretion of the NHS to determine the manner in which patient records are kept (i.e. whether this is computerised or otherwise). However, it also expressly acknowledges the rights of patients inherent in the Data Protection Act 1998, Human Rights Act 1998 and under the common law of confidentiality to control the extent to which their records are shared. Ultimately, it is for the patient to determine this and a patient can object to his or her records being made available to others, but this might have serious consequences for the ability of the NHS to provide care.

7.7 Information Sharing outside the NHS - There are many occasions when information needs to be shared outside the NHS, in addition to the occasions detailed above. Where possible, this information must be anonymous. However, this cannot always be achieved without reducing the level of patient care. In such cases we must observe the following:

1. The information is entrusted to the Trust. Therefore, if the information is shared elsewhere the person or organisation receiving it must maintain patient confidentiality

2. It continues to be the Trust's responsibility to ensure this information is protected; therefore we will need assurances from the recipient that this will be the case

7.8 Therefore it is important that the Trust establishes with whom, where and why we are sharing this information and what will happen to it once it leaves the Trust's care. Staff should seek assistance from the Caldicott Guardian or the Information Governance Service if they have any concerns or queries regarding those with whom we may need to share our patients' information.

7.9 Any clinical electronic reports produced that contains person identifiable information that are not directly to involved the care of the patient, the quality of the patient record or the clinical coding of the patient record must be anonymised/pseudonymised.

8. PROTECTING AND SECURING INFORMATION

8.1 Confidentiality applies not only to patient records, but also to information about the Trust and about staff. All this information should be handled with care and respect. Breaching confidentiality by improper use of health records, computer misuse or any other manner may lead to disciplinary action being taken. It could also call into question any professional registration and could lead to possible legal proceedings.

8.2 Keeping Information Private

8.2.1 The key principles are:

1. Not gossiping – this is an improper use of confidential information, whether it be about the Trust, colleagues or patients
2. Taking care when discussing cases in public places – there are occasions when it is important to discuss cases with colleagues for professional reasons. This can be to gain advice and to share knowledge and experience. Care must be taken to ensure that these discussions cannot be overheard. There would not be a need to reveal the identity of the patient concerned in most cases.
3. Social Engineering – be careful who you are giving information out to whether over the phone, face to face, email. A new term called Social Engineering has been introduced which basically means the art of manipulating people into performing actions or divulging confidential information. Always confirm the identity of the person you are speaking or writing to. Remember the IT department will never ask you to disclose your password to them.

8.3 Electronic Security of Information

8.3.1 Personal information must be kept secure. (Data Protection Act Principle 7). The IT New User Account Form must be completed and signed on commencement in post. This informs system manager(s) regarding who needs access to which systems and set users up accordingly. The form sets out the conditions of using information systems, email and the internet. If any member of staff breaches any of the regulations as set out in this form or this policy, he / she may face prosecution and / or disciplinary proceedings. Further information about the use of information systems, email and internet can be found in the IT Acceptable Use Policy.

All staff must:

1. Always log out of any computer system or application when work is finished
2. Personally owned memory sticks must not be used. The Trust has encrypted memory sticks and if you need one, you must apply for one. Please read the Removable Media Procedure for further Information

3. Never leave a computer logged on and unattended, even for the shortest of time – lock your screen if you need to move away from it for a short while (Ctrl, Alt and Delete to lock screen or windows symbol and 'L')
4. All portable equipment (laptops) must be registered with IT Services and must be encrypted
5. If portable media (for example CD / DVD) is to be used to transport / store personal identifiable and / or sensitive information, this must be encrypted. If you need to write to a CD / DVD this must be approved. Please read the Removal Media Procedure for further information. Never share / disclose logins / passwords with other staff. If other staff need to access systems, then appropriate access should be organised for them. If staff are found to be sharing passwords this may lead to a disciplinary action being taken in accordance with the Trusts disciplinary policy
6. Always store personal identifiable information onto a networked drive (for example U: Drive) not the local hard drive on the PC or laptop. If you need a network folder to be set up for you or your department to access, please contact IT Services
7. Staff should never look at any information relating to their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or with the patients' administration on behalf of the Trust
8. Do not use personally owned cameras or other technologies (such as cameras on mobile phones / Smartphone's) to take photographs for Trust purposes, for example, clinical photographs of patients. Please refer to the Clinical Photography Policy for further information.

8.3.2 The above list is not exhaustive and further information about acceptable use of IT systems and equipment can be found in the IT Acceptable Use Policy. Further information about Information Governance rules can be found in the Information Governance policies and procedures listed in the appendix and can be found on the Policy library page on the Trust intranet.

8.3.3 Some members of staff may be provided with a smartcard to access data on the national spine (National Care Record Service). The system also maintains a full audit trail of staff accessing records and data. The same principles apply to the use of smartcards as for logins and passwords.

8.3.4 Further information about Information Security and Information Governance can be found on the Information Governance pages and in the Information Governance policies located on the Trust Policy Library. If you are unsure about how to use, share, send personal and / or sensitive information, you must contact the Information Governance Service.

8.4 Manual / paper records

8.4.1 Manual / paper records, such as casenotes, must be:

1. Tracked if transferred using the Trust's tracking system. If staff require support regarding this, the Health Records library can be contacted or access the Health Records pages on the intranet
2. Returned to the filing location as soon as possible
3. Stored securely within office or clinic, so that the record can be found easily if needed urgently
4. Stored securely when not in use so that accidental viewing is prevented
5. Inaccessible to the public and left, even for the shortest of times, where they could be viewed by an unauthorised person

8.4.2 Patient records (Health Records and standalone notes) must not be taken off site unless there is a valid reason why this needs to happen. Please see the Health Records Policies and Procedures or your local policies and procedure regarding when this can occur. If a reason is not listed, approval must be obtained from the Caldicott Guardian.

8.4.3 Failure to adhere to Information Governance policies may result in monetary penalties being served by the Information Commissioners Office of up to £500,000. The Commissioner may impose a monetary penalty notice if a data controller (the Trust) has seriously contravened the Data Protection Act 1998 and if the contravention was of a kind likely to cause substantial damage or substantial distress.

8.5 Physical Security of assets

8.5.1 All staff must adhere to the IT Acceptable Use Policy regarding security of electronic equipment such as laptops and blackberries.

8.5.2 Staff working in an environment where any patient and / or staff records are kept must:

1. Shut / lock doors and cabinets and close windows
2. Wear ID badges at all times
3. Query strangers and inform the relevant security staff of suspicious activity

9. TRANSPORTATION OF INFORMATION

9.1 With several methods of communication now available to the Trust, safe haven principles ensure that information is communicated in the most secure way as possible with minimum risk.

9.2 Guidance regarding the secure transportation of personal identifiable and / or sensitive data using the telephone, fax and post can be found in the Safe Haven Procedure, and guidance can be found on the Information Governance Intranet Pages. Please refer to these for full details or ask the Information Governance Service

9.3 Please note if you are sending personal and / or sensitive information outside the UK and / or outside the European Economic Area, please inform the Information Governance department to ensure this is transferred safe and securely in compliance with the Data Protection Act principle 8 which states that personal information must not be transferred to other countries without adequate protection.

10. REQUESTS FOR PERSONAL INFORMATION

10.1 Requests for information may come from a variety of sources and it is dependant on the source and type of information requested as to how the request should be handled. Staff should never give out information on patients or staff to persons who do not have a right to access this information.

10.3 Access to health records

10.3.1 Patients may request access to their health records in compliance with Data Protection Act principle 6 which states that personal information must be processed in line with patients rights. Full details regarding this can be located in the Access to Health Records Policy.

10.4 Access to staff records

10.4.1 Staff may request access to their Human Resource records & personal file. Full details regarding this can be found in the Employee Personal Files: Storage, Retention and Disposal Policy.

10.5 Requests for information from the Police

10.5.1 When requests are received from the police, disclosure of information must be refused unless the data subject has given their consent for the information to be released or the appropriate documentation has been completed with the relevant signatures such as a Section 29(3). It is not enough to accept verbal consent. A consent form must be completed and signed by the data subject. Any data releases must be dealt with by the Access to Health Records Team. Personal information must not be disclosed to a third party such as a solicitor, police officer or officer of a court without the patient's express consent, unless it is required by law or can be justified in the public interest. Full details on disclosure can be found in the Access to Health Records Policy. There are a few occasions where the Police can insist on information being released for further information If in doubt, staff being presented with a request for disclosure from the police should seek further advice from the Trust's Legal Services Department, the Information Governance Service or the Caldicott Guardian.

10.6 Requests for information from the Media

10.6.1 During normal circumstances there is no basis for disclosure of confidential information to any sector of the media. However, there may be occasions when the Trust or individual staff may be asked for information about an individual patient or relative of the patient. Examples include:

1. Requests for updates on the condition of a particular patient, such as a celebrity or local politician
2. After a major incident – such as a road traffic accident
3. Circumstances where a patient, or relative of a patient, is complaining publicly regarding the treatment and care provided by the Trust.

10.6.2 All communication with the media must be directed to the Trust's Communications Manager.

10.6.3 Requests for personal information may also come into the Trust from other sources. Please contact the Information Governance Service for advice before disclosing any information to any organisation.

11. RETENTION AND DISPOSAL OF INFORMATION

11.1 Principle 5 of the Data Protection Act states that personal information must not be kept longer than necessary, When disposing of confidential waste, staff must use a Shred-IT console and / or a cross cut shredder (not single cut) provided by the Trust.

11.2 When disposing of IT equipment or removable computer media, IT Services should be contacted. Deleting information from a system does not necessarily mean the data has been removed from the hard drive. Before hard drives are disposed of personal and / or sensitive data must be removed by IT Services. For further details contact IT Services.

11.3 Both health records and non-health records have assigned minimum retention periods as classified in the Records Management: NHS Code of Practice.

12. INCIDENT REPORTING

12.1 It is imperative that all incidents or near misses relating to the handling of confidential data and / or information security are recorded and reported as soon as possible. This vital feedback allows the Trust to learn from past experience and prevent incidents of a similar nature being repeated.

12.2 Incident reporting is not about "getting people into trouble" as it aims to create an open environment where improvements can be made. If staff have a concern in regard to confidentiality and / or information security they should raise this within the Trust. Employees making a disclosure to the Trust will be protected where they have an honest and reasonable suspicion that the wrongdoing has occurred, is occurring or is likely to occur. Please read the Trust's Open Door Policy for Handling Staff Concerns for further information.

12.3 Concerns in regard to any potential or actual breaches in confidentiality and / or information security are reportable occurrences and must be reported as soon as possible using DatixWeb to report such incidents. Full details can be found in the Trust's Incident Reporting Procedure and Information Governance and Information Security Incident Reporting Procedure (both located on the Trusts policy library)

13. TRAINING AND IMPROVING KNOWLEDGE

13.1 It is a compulsory requirement for staff to complete induction training on commencement in post. Information Governance compulsory e-learning training must be completed annually to ensure that staff are fully informed regarding the latest developments within Information Governance. Staff with IG roles must undertake designated modules on the Information Governance Training Tool provided by NHS Connecting for Health.

13.2 Staff within the Trust are encouraged to be proactive and ask questions if they are unsure about any issues associated with holding, using and sharing personal identifiable and / or sensitive information. Information risk assessments relating to information governance must be produced so these can be investigated and any appropriate action taken to mitigate any potential incidents.

14. SOCIAL NETWORKING / MEDIA

14.1 Please refer to the IT Acceptable Use Policy regarding use of social networking sites.

15. AUDITING

15.1 Confidentiality auditing will focus primarily on control within electronic records management systems but also includes paper record systems and confidentiality processes undertaken by departments / wards, for example safe haven processes. The purpose is to discover whether confidentiality has been breached or put at risk through deliberate misuse of systems as a result of weak, non-existent or poorly applied controls. Assurance that controls are working should be part of the Trust's overall assurance framework.

15.2 Staff emails and internet use are also monitored by the Trust. Inappropriate access or misuse may result in disciplinary action. For further information, please read the IT Acceptable Use Policy.

15.3 Failure to follow Information Governance policies and utilise information security standards available to staff (such as encryption) to safeguard confidentiality may result in a breach. This contravenes the Data Protection Act 1998, the Computer Misuse Act 1990, the Human Rights Act 1998 and the Confidentiality: NHS Code of Conduct.

16. NON-COMPLIANCE

16.1 All staff agree to uphold confidentiality on signing their contract of employment and this Confidentiality Code of Conduct. This agreement continues after employment.. Non-compliance with this code may result in disciplinary action being taken in accordance with the Trust's Disciplinary Procedures and in line with the NHS Care Record Guarantee. The guarantee states that the NHS will keep a record of everyone who accesses the electronic information on the NHS Care Records Service and members of the public can ask for a list of everyone who has accessed their records.

16.2 Under section 55A to 55E of the Data Protection Act 1998 (the "Act"), introduced by the Criminal Justice and Immigration Act 2008, the Information Commissioner can serve a monetary penalty on a Data Controller such as the Trust up to £500,000. In addition, the Privacy and Electronic Communication (EC Directive) (Amendment) Regulations 2011 inserted sections 55A to 55E into the Privacy and Electronic Communication (EC Directive) Regulations 2003, enabling the Commissioner to serve a monetary penalty notice on anyone who breaches the 2003 Regulations. Further information can be found on the ICO website (ww.ico.gov.uk).

16.3 The disciplinary procedure and the NHS Care Record Guarantee can be located on the Trust intranet site. Staff should also be aware that they may become personally liable in the civil courts for any breach of confidence that occurs after work for the Trust ends.

17. WHISTLE BLOWING (Open Door Policy for Handling Staff Concerns)

17.1 If staff have issues or concerns regarding the use of personal identifiable and / or sensitive information, confidentiality and / or information security, staff can raise this issue using the Whistle Blowing Policy (Raising Concerns Policy). The principle aim of this policy and procedure is to encourage and enable employees to raise concerns regarding the delivery of care or services, or the running of the Trust business, in a responsible way and to have the issue satisfactorily resolved within the Trust.

17.2 Individual members of staff have a duty to raise with their manager, or staff side representative, any matters of concern they may have about the delivery of care or services, or the running of the Trust's business.

17.3 This policy aims to supplement, rather than remove, this obligation as well as any professional responsibility individuals may have under codes of conduct, etc. The Trust would expect all employees to fully exhaust the Raising Concerns Policy before raising the issues with outside persons, bodies or authorities (Please refer to Sections 7 and 8). However, this will not apply where the Trust has made special arrangements, for example, Fraud Hotline. The policy can be located on the Trust policy library on the intranet.

References and further information **Appendix 1**

Policies & Procedures

1. IG Policies and Procedures
2. Human Resources Policies and Procedures

Wrightington, Wigan and Leigh NHS
NHS Foundation Trust

CONFIDENTIALITY CODE OF CONDUCT AGREEMENT

Your personal responsibility concerning confidentiality and security of information (relating to patients, staff and the organisation)

Please note that the full Confidentiality Code of Conduct should be read and understood prior to this disclaimer document being signed. If there is anything that is not clear please contact your manager.

The following form is for all staff to sign which includes:
Staff, volunteers and individuals undertaking a contract for services to the Trust e.g. Contractors & Agency staff.

During the course of your time within the Trust, you may acquire or have access to confidential / personal and / or sensitive 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, its patients and employees. Such information may relate to patient records, Trust business, electronic databases or methods of communication such as use of fax machines, hand-written notes made containing patient information etc. If you are in doubt as to what information may be disclosed, you should check with your manager.

The Data Protection Act 1998 regulates the use of computerised information and paper records of identifiable individuals (patients and staff). The Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal and / or disciplinary action.

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

EMPLOYEE'S NAME:		**MANAGERS NAME**	
TITLE:		**TITLE:**	
DEPARTMENT AND DIVISION:		**DEPARTMENT AND DIVISION:**	
SIGNATURE:		**SIGNATURE:**	
DATE:		**DATE:**	

A COPY OF THIS SIGNED FORM SHOULD BE RETAINED IN THE EMPLOYEE'S PERSONAL FILE.

Glossary of Terms (relevant to Policy) **Appendix 3**

Confidential - The Oxford English dictionary definition of confidential is `intended to be kept secret` (2002).

Personal Identifiable Information / Data (PID) - This is anything that would enable that person's identity to be established by one means or another e.g. name, address, date of birth, NHS Number, National Insurance number and photographs

Sensitive information - This can be broadly identified as that which if lost, misdirected or compromised could affect individuals, organisations or the wider community.

Safe Haven - The term `Safe Haven` is a location (or equipment) that is situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.