Reference Number and Policy name: Confidentiality Code of Conduct for staff	**Version:** **1.0 Sept 2012**		**Status: Final**	**Author: IG Officer** **Director Sponsor: Medical Director**

Version / Amendment History	Version	Date	Author	Reason
	V0.1	April 12	IG Lead	Creation
	V0.2	June 12	IG Lead	Consultation with Governance department
	V0.3	June 12	IG Lead	Trust Wide consultation and with Policy committee members
	V 1.0	**Sept 12**	**IG Lead**	**New Policy approved TMT**

Intended Recipients: All staff	
Consultation Group / Role Titles and Date: IGSG, Trust Wide, Policy Committee Members	
Name and date of Trust level committee where reviewed	Policy Committee September 2012
Name and date of final approval committee	TMT September 2012
Date of Policy issue	September 2012
Review Date and Frequency [standard review frequency is 3 yearly unless otherwise indicated]	3 years September 2015
Training and Dissemination: Policy will be placed on the Trust intranet and all staff informed via an AUB. Staff will complete annual Mandatory Information Governance Training.	
To be read in conjunction with: CP06 Consent Policy OP30 Policy on Research Governance OP41 Induction and Mandatory Training Policy.	

OP85 Information Sharing Policy Records Management Strategy OP13 Information Governance Policy OP12 Information Security Policy Information Governance Strategy	
Initial Equality Impact Assessment [all policies]: **Completed Yes** **Full Equality Impact assessment [as required]:** **Completed NA**	
Contact for Review	Information Governance Lead
Implementation plan / arrangements [Name implementation lead]	Information Governance Lead
Monitoring arrangements and Committee	IGSG
Document summary / key issues covered: Confidentiality compliance to law and guidance. Expectations of staff for maintaining confidentiality. Maintaining confidentiality in practice, guidance on disclosing information to others. Safe haven procedures for sharing information by phone, fax, post and manual transfers. Consequences of failure to maintain confidentiality.	

VALIDITY STATEMENT

This document is due for review on the latest date shown above. After this date, policy and process documents may become invalid. The electronic copy of this document is the only version that is maintained. Printed copies must not be relied upon to contain the latest updates and amendments.

Contents

Sections	**Page**
1.0 Policy Statement	4
2.0 Definitions	5
3.0 Accountabilities	5
4.0 Policy Detail	
Law and guidance related to confidentiality (for information)	6
Accountabilities- All staff	6
4.1 Practical Guide to Legal Framework for disclosure of information	6
4.2 What patients have a right to know	6
4.3 When is it lawful for me to share information?	6
4.4 Disclosing information for care (staff, other NHS and patients family)	6
4.5 Disclosing information for other medical purposes	6
4.6 Disclosing information for reasons other than care	6
4.7 Information requests from police	6
4.8 Information requests from media	6
4.9 Sharing information safely by post, phone, fax, transport (safe havens)	6
4.10 Failure to maintain confidentiality	6
4.11 Police data request- Section 29(3) Data Protection example form	6
4.12 Safe haven flow charts	6
4.13 Example Courier log	6
5.0 Financial Risk assessment	6
6.0 Equality Impact Assessment	6
7.0 Maintenance	6
8.0 Communication & Training	7
9.0 Audit process	7
10.0 References	8

1.0 Policy Statement [Purpose / Objectives of the policy]

The purpose of this code is to ensure everyone working within The Royal Wolverhampton NHS Trust (The Trust) is aware of their responsibilities when using confidential information and maintains the correct relationship with patients, staff and others while carrying out the business of the Organisation.

All staff working in 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, for health and other professionals, through their own professions' Code(s) of Conduct.

For the purpose of this code all data or information that can be related to an identifiable person is considered confidential; this includes patient and staff data, and must only be used in line with this guidance and the law.

Staff may also come into contact with confidential non-person identifiable information, including for example commercially sensitive data or reports about the organisations business, which should be treated with the same degree of care.

The principle behind this Code of Practice is that no member of staff shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trusts security systems or controls in order to do so.

This Code has been written to meet the requirements of and inform staff about:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The legal framework governing confidentiality
- Staffs individual responsibilities with regard to compliance with the law
- The information that is confidential
- How to ensure information remains confidential
- The systems and processes for protecting personal information
- The circumstances under which confidential information can be disclosed
- Who to approach in the Trust for assistance with disclosure issues
- Possible sanctions for breaches of confidentiality
- Secure transfer of information

A full list of Legislative requirements for the correct use and governance of information can be found in Attachment 1

This Code has been produced to protect staff by making them aware of the correct procedures and to minimise the risk of an inadvertent breach of any of these requirements.

2.0 Definitions

Confidentiality- is 'the entrusting of private matters to a person with reliance on their fidelity or competence' (The Oxford English Dictionary, Second Edition)The notions of trust and competence are vital. All employees are responsible for maintaining the confidentiality of information gained during their employment with the Trust.

Personal identifiable information/data - Is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, Telephone Number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual this includes any person including patients, visitors, staff.

Sensitive information – Means any category of information legally defined as particularly sensitive relating to racial or ethnic origin, political or religious beliefs, physical, mental or sexual health, any offences or proceeding relating to the individual, trade union membership, information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy, information relating to safeguarding vulnerable individuals.

Safe Haven - is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-indefinable information can be held, received and communicated securely.

3.0 Accountabilities

This policy applies to all staff, and external contractors who are employed to carry out work on behalf of The Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for confidentiality of information and safe transfer of information

Please see Attachment 2 for a full list of accountabilities for the Trust board, specialist staff and contractors.

All staff:

- Treat all information in the strictest confidence
- Store all information safely when not in use, and destroy all out of date information securely, reference should be made to the Records Management Strategy for destruction schedules
- Wherever possible use anonymised information rather than person identifiable information and only disclose information for justifiable purposes
- Only give information to those individuals who need to know that information and ensure that any individual, to whom information is given,

has a legitimate right to receive it- Always use safe haven processes when dealing with personal data by phone, fax, transport. Appendix 1

- Follow security procedures outlined in OP12 Information Security Policy for keeping information including; ensuring computers are locked when you are not using them, keeping access controlled areas secure and not sharing passwords with anyone else.
- Be vigilant of where conversations take place to prevent unintentional disclosure of information through overheard conversations
- Always report incidents relating to breaches of confidentiality verbally via the incident reporting process and to your Line Manager, Information Governance Lead. Any breaches in confidentiality must be reported in line with OP10.Risk Management Reporting Policy

4.0 Policy Detail

Law and guidance related to confidentiality (for information)	Attachment 1
Accountabilities- All staff	Attachment 2
4.1 Practical Guide to Legal Framework for disclosure of information	Attachment 3
4.2 What patients have a right to know	Attachment 4
4.3 When is it lawful for me to share information?	Attachment 5
4.4 Disclosing information for care (staff, other NHS and patients family)	Attachment 6
4.5 Disclosing information for other medical purposes	Attachment 7
4.6 Disclosing information for reasons other than care	Attachment 8
4.7 Information requests from police	Attachment 9
4.8 Information requests from media	Attachment 10
4.9 Transferring/Sharing information safely by post, phone, fax, transport (safe havens)	Attachment 11
4.10 Professional responsibility to maintain confidentiality	Attachment 12
4.11 Seven Golden Rules for information sharing	Attachment 13
4.12 Police data request- Section 29(3) Data Protection example form	Appendix 1
4.13 Safe haven flow charts	Appendix 2
4.14 Example Courier log	Appendix 3

5.0 Financial Risk Assessment

A financial risk assessment has been undertaken and no financial risks have been identified as a result of implementing this policy.

6.0 Equality Impact Assessment

An assessment has been undertaken, no adverse affects have been identified for staff, patients or the public as a result of implementing this policy.

7.0 Maintenance

This policy will be reviewed every 3 years or sooner if changes in legislation or guidance require. Responsibility lies with the Information Governance Steering Group.

8.0 Communication and Training

Approved Trust policies will be made available to staff via the Trusts intranet page.

All staff are required to complete Information Governance Training on an annual basis via Trust Induction and/or Mandatory training days. Please see OP41 Induction and Mandatory Training Policy. Where necessary to support specific roles and responsibilities a training needs analysis shall be reviewed by the IGSG

This policy will be implemented and communicated through the work of the Information Governance Steering Group. An assessment of compliance with the requirements of the IGToolkit will be undertaken each year. The Policy will be also implemented by the Information Governance Strategy which will set standards and a framework for monitoring.

9.0 Audit Process

Criteria	Lead	Monitoring method	Frequency	Committee
IGToolkit sign off- confidentiality requirements	Medical Director	Report	Annual	Trust Board/ TMT
IGToolkit compliance - confidentiality requirements	Medical Director	Online evidence submission	3 times annually	IGSG
Incidents and breaches- IG Confidentiality	IG Lead	Report	Bi monthly	IGSG
Informing patients how their information will be used	Authors of patient information leaflets	Review of patient information leaflets	Upon leaflet review dates	Patient information Committee
Informing patients how their information will be used	Data Protection Officer	Update of the Trust fair processing notice- via Data Protection Officer	Ad Hoc	IGSG

Disclosing information	IG Lead	Update and review of Register of information sharing agreements	Ad Hoc	IGSG
Police requests	Health Records Managers	Report on number of police request made, those upheld/declined	Quarterly	Health Records Committee

10.0 References

The Royal Wolverhampton NHS Trust Policies and Strategies:

Policies

CP06 Consent Policy.

CP18 Clinical Photography, Video and Audio Recordings

OP07 Health Records Policy

OP13 Information Governance Policy

OP12 Information Security Policy

OP14 Content of Health Records

OP30 Policy on Research Governance

OP41 Induction and Mandatory Training Policy.

OP85 Information Sharing Policy

Strategies

Records Management Strategy

Information Governance Strategy

Other sources

Definition of confidentiality used. The Oxford English Dictionary. Second Edition. (1989).Northamptonshire. Oxford University Press.

Department of Health (2010).The NHS Confidentiality Code of Practice <http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550 >

Department of Health (2010).Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures <http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_122012>

National Information Governance Board (2011) The NHS Care Record Guarantee for England (version 5) < http://www.nigb.nhs.uk/pubs/nhscrg.pdf >