Heart of England NHS
NHS Foundation Trust

Confidentiality Policy and Procedure V6.0

This policy sets out the required standards for all Trust employees:

- To ensure compliance with statutory, national and local requirements through the application of legislation and best practice
- To ensure patients, staff and members are aware how their information may be used and, where reasonable, respect conditions requested by individuals to limit the use of their information
- To establish clear lines of accountability to protect information and support staff in the provision of a confidential service;
- To integrate confidentiality into the Trust's risk management process to minimise accidental disclosure and address issues associated with security or confidentiality of information;
- To facilitate information sharing arrangements between NHS Trusts, social care and other relevant organisations;
- To ensure valid implied or explicit consent is obtained prior to disclosure;
- To establish clear lines of accountability to authorise the disclosure of confidential information.

Paper Copies of this Document

- If you are reading a printed copy of this document you should check the Trust's Policy website (**http://sharepoint/policies**) to ensure that you are using the most current version.

Ratified Date: January 2013
Ratified By: Information Governance Committee
Review Date: January 2016
Accountable Directorate: Corporate Affairs

Meta Data

Document Title:	Confidentiality Policy and Procedure
Status:	Active
Document Author:	Information Governance Manager
Accountable Director:	Director of Corporate Affairs
Source Directorate:	Corporate Affairs
Date Ratified	January 2013
Date Of Release:	January 2013
Review Date:	January 2016
Related documents	ICT Policy and Procedures Information Governance Policy Incident reporting policy Access to Medical Records Procedure Safe HavenPolicy and Procedure Risk Management Policy and Procedures Records Management Policy HR Policies and Procedures RA Policy and Procedures Patient Information Strategy Photographic and Video Recording Consent and Confidentiality Policy Safeguarding Adults Policy Consent to Examination or Treatment Policy Freedom of Information Policy and Procedure Code of Conduct
Relevant External Standards/ Legislation	Information Governance Toolkit standards Data Protection Act 1998 Freedom of Information Act 2000 NHS: Confidentiality Code of Practice 2003 CQC Regulations NHSLA Regulations NHS Cancer Screening Programme: Confidentiality and Disclosure Policy
Stored Centrally:	Electronic copy on Intranet site

Revision History

Version No.	Date of Release	Document Author	Ratified by	Date Ratified
1.0	Aug 07	Information Governance Manager	IGC	Aug 07
2.0	Feb 08	Information Governance Manager	IGC	Feb 08
3.0	Feb 10	Information Governance Manager	SW	Feb 10
4.0	Aug 11	Information Governance Manager	SW	Aug 11

5.0	April 2012	Information Governance Manager	SW	April 12
6.0	Nov 2012	Information Governance Manager	IGC	Jan 2013

Contents

1 Circulation

This policy, and associated procedures, applies to all staff employed by the Heart of England NHS Foundation Trust including temporary, locum, volunteer, and contract staff.

2 Scope

All employees working in the NHS are bound by a legal duty of confidence to protect personal and sensitive 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, in addition, through professional Codes of Conduct.

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Patients generally have the right to object to the use and disclosure of confidential information that identifies them, even if this has implications for their healthcare.

However, in certain circumstances, confidential patient information may be disclosed to the police and other organisations without the patient's consent.

In most cases, where it is reasonably possible, explicit consent will be obtained from the patient before disclosure of confidential information.

The exceptions to this approach are when the Trust is legally obliged to disclose information without the consent of patients.

Examples of this are as follows:

Legal Duty: (Disclosure, even without consent)

- Prevention of Terrorism Act (1989) and Terrorism Act (2000)
- The Road Traffic Act (1988)
- Data Protection Act 1998

The Police may seek personal information under an exemption of the Data Protection Act 1998. *A Section 29(3) exemption* is used when making enquires which are concerned with:

a) The prevention and detection of crime or
b) the apprehension or prosecution of offenders

The Police will need to produce a Section 29(3) form requesting the information, which has been signed by a Police Inspector.

Public Interest:
Information may be disclosed without the patients consent if it is in the public interest for disclosure.

Section 60: Health and Social Care Act
A request for the disclosure of confidential patient information without the patients consent can also be undertaken by using a Section 60 request form as part of The Health and Social care Act, section 60. Further information can be found at Guidance notes: Section 60 of the Health and Social Care Act 2001: Department of Health - Publications and statistics

3 Definitions

Confidential information
A duty of confidence arises when one body discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. In the context of this policy confidential information can be;

- personal or sensitive information supplied on this basis to the Trust from patient, staff or member, or
- Information supplied under contractual arrangement from another body or organisation.[1]

Personal information
The legal definition of personal information, defined in the Data Protection Act, 1998 is listed at Attachment 1, however for the purpose of this policy the broader concept outlined in the Caldicott report is a more useful definition.

*"…there are many items of information which could be used to identify individual patients. Although particular items may not in themselves uniquely identify an individual patient, taken together they may permit identity to be inferred. Different combinations of items may require different degrees of effort…**all** items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients to a greater or lesser extent'.*

Sensitive information
The precise meaning of sensitive information, also listed at Attachment 1 can be summarised as personal information including about any aspect of:

- Racial/ethnic origin
- Religious or other beliefs
- Physical or mental health
- Sexual life
- Commission or alleged commission of offences
- Political opinions or trade union membership

Information in this context may be written, spoken or otherwise recorded through the use of photography or medical imaging regardless of storage media. It also includes clinical samples where they may be used to extract personal or sensitive information.

For the purpose of this policy, the Trust also applies the additional definitions:

Healthcare purposes:	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.[2]
Patient information[3]:	All patient information, in whatever form, provided to, created or used

[1] The Freedom of Information Act classes information as provided in confidence if 'disclosure to the public (otherwise than under this Act) by the public authority holding it would constitute a breach of confidence actionable by that or any other person.
[2] DH – Confidentiality: NHS Code of Practice November 2003
[3] Including information regarding the deceased

	by or for the Trust for the purpose of Healthcare or Healthcare administration. This will include both personal and sensitive information.
Staff information:	All staff information in whatever form, provided to, created or used by the Trust for the purpose of staff employment or management. This will include both personal and sensitive information. Information provided for the purpose of becoming a Member of Heart of England Foundation Trust. It will mainly refer to personal information but where provided may include sensitive information such as ethnicity or lifestyle information.
Explicit Consent:	This means articulated agreement and relates to a clear and voluntary indication of preferences or choice. It is usually given orally or in writing and in circumstances where the available options and the consequences have been made clear.
Implied consent:	This means assent or agreement that has been signalled by the behaviour of an informed individual.

4 Reason for Development

Patients, staff, members and the general public have a right to expect that the Trust is a confidential environment in which their information will be treated with due care and respect, shared only with their consent, in their best interests or through a legislative duty.

Similarly suppliers of services or goods to the Trust have a right to expect that contractual confidentiality agreements will be honoured subject to existing and subsequent legislative limitations.

The Trust is committed to achieving National standards of best practice and fully endorses the Confidentiality: NHS Code of Practice which builds upon the recommendations of the Caldicott Committee to describe a confidential service and define practice required to achieve this. The Trust also embraces a culture of openness and seeks to proactively facilitate the public's 'right to know'.

The Trust recognises its fundamental responsibility to patients, staff and members to ensure the confidentiality and security of personal or sensitive information in all of its information processes. Furthermore it has a responsibility to balance the interests of the public, patients, staff and members when disclosing confidential, personal or sensitive information for purposes other than for which it was supplied. In particular, patient information for purpose other than Healthcare or to non NHS bodies.

The Trust has a statutory obligation to comply with legislation and national policy on the management, security and disclosure of confidential information. Principally:

- Confidentiality: NHS Code of Practice 2003
- The Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2000

- Access to Medical Records Act 1990
- Access to Medical Reports Act 1988
- Administrative Law
- Common law on confidentiality

5 Aims and Objectives

The aims and objectives of this policy are:

- To ensure compliance with statutory, national and local requirements through the application of legislation and best practice;
- To ensure patients, staff and members are aware how their information may be used and, where reasonable[4], respect conditions requested by individuals to limit the use of their information;
- To establish clear lines of accountability to protect information and support staff in the provision of a confidential service;
- To integrate confidentiality into the Trust's risk management process to minimise accidental disclosure and address issues associated with security or confidentiality of information;
- To facilitate information sharing arrangements between NHS Trusts, social care and other relevant organisations;
- To ensure valid implied or explicit consent is obtained prior to disclosure;
- To establish clear lines of accountability to authorise the disclosure of confidential information.

6 Standards

- Patient, staff and member information, whether electronic or manual, should be secure, appropriately accessed, transferred and ultimately disposed of in line with the Trust's Data Protection policy[5];
- Patient information should only be shared for the purpose of healthcare in line with Trust guidance and procedures on information sharing;
- Transfer of personal and sensitive information should adhere to the principles of a Safe Haven in line with the Trust's Safe Haven procedure[6];
- All new contracts for the provision of goods or services must include a confidentiality statement in line with this policy, national legislation and common law;
- Personal and sensitive information will be disclosed in line with the principles of the NHS code of practice;
- Individuals will be provided with access to information held about them in accordance with legislation and Trust guidance on:

    - Access to medical records/reports (see Access to Health Records Policy)
    - The Data Protection Act

- The Trust will implement processes to enable it to share information safely with other NHS organisations for the purpose of healthcare on the basis of a patients implied consent;

[4] provided the conditions do not compromise the Trusts ability to provide safe clinical care.
[5] Outlines Human Resources process to manage staff requests for their personal information
[6] see attachments 5-9

7 Responsibilities – Individuals

7.1 Chief Executive

The Chief Executive retains overall responsibility to the Trust Board for overseeing an appropriate infrastructure to ensure the provision of a confidential and safe service. He/she delegates operational responsibility to the Director of Corporate Affairs.

7.2 Director of Corporate Affairs

The Director of Corporate Affairs is responsible to the Trust Board and Chief Executive in relation to confidential information and will provide reports to the Trust Board in this regard. With the assistance of other senior managers within the Trust he/she will oversee a programme of activities to ensure the provision of a confidential service and authorise remedial action when required to protect information.

7.3 Caldicott Guardian

TheCaldicott Guardian has particular responsibility for ensuring the appropriate disclosure of patient information and where required will become directly involved with the decision to disclose or withhold information.

7.4 Senior Information Risk Owner (SIRO)

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the Trust's Information Asset Owners, Information Governance Manager, the Trust's Information Security Manager, and the Trust's Caldicott Guardian, although ownership of the Information Security Risk Management Policy and risk assessment process will remain with the SIRO.

7.5 Information Governance Manager

The Information Governance Manager is responsible for the development and review of this policy in line with national requirements and legislation. He/she will liaise with other key staff within the Trust to support the continued development and regulation of processes to support the implementation of this policy.
Supported by the Information Governance team he/she will:

- provide advice and support for all staff on issues relating to Confidentiality;
- oversee the investigation of adverse incidents in relation to the accidental or inappropriate disclosure or loss of confidential information;
- have day to day responsibility for the management of non-routine or Police requests for personal or sensitive information;
- develop and deliver a variety of training packages and resources for all staff regarding the management, security and disclosure of confidential information;
- support development of the infrastructure and resources to enable effective informed consent;
- liaise with external organisations to develop appropriate information requesting processes and information sharing safeguards;
- advise upon wider lessons learnt through the management of information requests.

The Trust Information Governance Manager will be responsible for ensuring that the Trust complies with national reporting requirements (currently through the Information Governance Toolkit and

Care Quality Commission Regulations). He/she will provide regular reports to the appropriate committees as required on all issues relating to this policy.

7.6 Director of ICT

Through the Head of ICT and Medical Records Department, the Director of ICT will oversee the development of supporting policies and processes to maintain the confidentiality of manual and electronic patient Information and manage routine requests for the disclosure of this information.

He/she will be operationally responsible for ensuring compliance with this policy in the areas of his/her responsibility; in particular, the Trust's Medical Records Libraries and centralised electronic patient information Management systems. He/she will provide regular reports to the Trust Committees, as required, on all issues that may affect the management, security or disclosure of confidential patient information.

7.7 Director of HR and Organisational Development

The Director of HR & Organisational Development will oversee the development of supporting policies and processes to maintain the confidentiality of manual and electronic staff Information and manage routine requests for the disclosure of this information.
He/she will provide regular reports to the Trust Committees, as required, on all issues that may affect the management, security or disclosure of confidential staff information.

7.8 Operations Directors and Clinical Directors

Operations Directors and Clinical Directors are responsible for the local implementation of this Policy. They will be responsible for:

- development of effective local processes to ensure the appropriate management, security and disclosure of confidential information;
- identification of key personnel responsible for the coordination of local processes and appropriate liaison with the Information Governance Manager;
- identification of training requirements for all staff involved in the management, security or disclosure of confidential information;
- management of issues preventing compliance with this policy through the Trust Risk Management processes.

7.9 All Staff

All staff have a responsibility to ensure that they are aware of, and comply with this policy and procedures.

Staff must adhere to the principles of the Data Protection Act 1998, common law on confidentiality and other relevant legislation in all dealings with, or when disclosing to external agencies, **any** personal, sensitive or otherwise confidential information. Where disclosure is not covered by local procedure they are responsible for seeking the advice of the Information Governance Manager.

8 Board and Committee responsibilities

8.1 Trust Board

The Trust Board is responsible for assuring that the Trust has appropriate Information Governance systems to enable the organisation to deliver its objectives and statutory requirements.

8.2 Governance and Risk Committee

The Governance and Risk Committee is responsible for overseeing the Trust's Governance work program. Through the Information Governance Committee it will be responsible for monitoring progress with the implementation and delivery of this policy.

8.3 Information Governance Committee

The Information Governance Committee is responsible for ensuring the development, review and implementation of this and supporting policies. The Committee will:

- review and monitor activity to deliver this policy;
- advise on issues which may prevent implementation or compliance;
- review incidents which breach this policy;
- review and monitor the number and type of information requests;

As appropriate, it will advise the Governance and Risk Committee of issues of concern in relation to the management, security and disclosure of confidential information.

The Committee is also responsible for the review and ratification of the Trusts annual submission to the Information Governance Toolkit.

8.4 Medical Records Committee

The Medical Records Committee will advise upon the implementation of this policy in the Medical Records libraries and electronic patient information management systems (e.g. iCare, HISS).

9 Training Requirements

The Information Governance Manager and Director of Corporate Affairs will ensure provision of training for relevant staff to enable them to understand and carry out their responsibilities relating to disclosure of confidentiality. This will be achieved through the Department of Health's Information Governance Training Tool and the following:

- awareness training at corporate induction for new staff on all aspects of confidentiality;
- detailed training on the principles of the Data Protection Act as part of local induction for key personnel including junior doctors, nursing and medical records staff;
- follow-up/refresher training, where requested, or to reflect key changes in legislation, local or national guidance.

10 Monitoring and Compliance

This policy will be monitored by the Trust on a quarterly basis through reports from the Information Governance Manager to the Information Governance Committee.

Heart of England NHS
NHS Foundation Trust

Attachment 1: The Data Protection Act Principles

The Data Protection Act defines **eight principles** put in place to make sure that personal or sensitive information is handled properly.

These state that data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept for longer than is necessary
6. processed in line with your rights
7. secure
8. not transferred to countries without adequate protection.

By law, data controllers have to keep to these principles.

The Data Protection Act 1998 makes the following definitions:

"personal data" means data which relate to a living individual who can be identified-

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"sensitive personal data" means personal data consisting of information as to-

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Heart of England NHS
NHS Foundation Trust

Attachment 2: Procedure for responding to request for patient identifiable information without consent.

Examples of such requests include requests from the Coroner, Police or other external bodies.

The *Protocol for releasing patient information without consent under section 29(3) of the Data Protection act 1998 – Prevention and detection of crime* is at Attachment 10. This should be followed for all police requests. For all other requests the procedure below should be followed.

On receipt of a request, contact the Information Governance Manager with details of the request, including:

- name and organisation of enquirer, contact number
- name and PID of patient,
- summary of request including reason for request
- date of request
- any documents sent to you e.g. *Court Order.*

The Information Governance Manager will record all requests and ensure that disclsoure of information is acceptable and practicable within the bounds of Trust procedures and legal requirements.

Once approval from the Information Governance Manager is gained, information can be disclosed.

If the information cannot be disclosed the Information Governance Manager will provide an explanation, and where necessary issue a refusal notice.

Contact Details: Information Governance Manager, Corporate Affairs Directorate, Heart of England NHS Foundation Trust, Bordesley Green East, Birmingham, B9 5SS publication.scheme@heartofengland.nhs.uk

Heart of England NHS
NHS Foundation Trust

Attachment 3: Protocol for releasing patient information without consent under section 29 (3) of the Data protection Act 1998 – Prevention and detection of crime

Data Protection Act 1998 – Prevention and Detection of Crime

Patient information in the NHS is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of exceptions to this rule, and this protocol addresses the release of information to the police under Section 29(3) of the Data Protection Act 1998 for the purpose of preventing and detecting crime. Although developed with West Midlands Police this protocol should also be followed when dealing with requests from other law enforcement agencies such as Department of Work and Pensions and UK Border Agency.

Whilst the police have no general right of access to healthcare records, Section 29(3) is a discretionary exemption that may allow the release of information for the prevention and detection of crime. Application of this exemption should be on a case by case basis and it is for the data controller (the Trust) to decide if failure to disclose the information is likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. Therefore it is for the data controllers within the NHS to decide when it is appropriate to disclose personal data and in the case of sensitive personal data heightened criteria for such disclosures apply.

The NHS Code of Confidentiality explains that Trusts are "permitted to disclose personal information in order to prevent and support detection, investigation and punishment of **serious** crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service."

In this situation serious crime is defined as murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm and all such crime may warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Where the Trust considers that disclosure is justified it will be limited to the minimum necessary to meet the need and patients should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk.

In the absence of a requirement to disclose there must be either explicit patient consent or a robust public interest justification and this decision should be made by the Trust's Caldicott Guardian. What is or isn't in the public interest is ultimately decided by the Courts and where a court order is obtained then Section 35(1) would apply which is an absolute exemption and compliance by the data controller is compulsory.

Data Protection Act S29(3): Law Enforcement Request for Healthcare Information

When a member of West Midlands Police (or any other law enforcement agency) requires healthcare information from the Trust and the patient has not given their consent for the release of information then an application under S29(3) of the Data Protection Act should be made.

West Midlands Police have a pro forma that should be used to make the request, a copy of which is attached to this protocol. As a minimum the request should include:

- Name and collar/warrant number of requester
- Contact number
- Address of police station
- Date of request
- Authorising signature of an Inspector or above
- Clear statement of what is wanted and the crime that is being investigated

Under no circumstances will information be supplied to any law enforcement agency on an ad hoc or informal basis.

Completed application forms should be sent to the Trust's Information Governance Office on the secure fax number **0121 424 3919**

The Trust will acknowledge the request and state the timescale by which time they will provide a response. Under the Data Protection Act 1998 the Trust has 40 days to respond to a request for information but will endeavour to provide a response as soon as possible.
For further information on this process you may telephone:

NHS HEART of ENGLAND NHS Foundation Trust	**HEFT Information Governance** **0121 424 2549/2629**
	West Midlands Police **0845 113 5000**
	Information Commissioners Office **01625 545745**

WA 170
(amended 12.04)
(Word 97)

WEST MIDLANDS POLICE

Telephone: **0845 113 5000***
Extension: (8 digit code)
Direct Line:
Please Ask For:
Station/Department:
Crime Reference No:
Facsimile:
Email: @west-midlands.pnn.police.uk

Crime Stoppers: 0800 555 111
Our Reference:
Your Reference:

DATA PROTECTION ACT 1998 – Request for Disclosure of Personal Data Under section 29(3) of the Data Protection Act 1998

In order to maintain Police Confidentiality you are requested not to inform the Data Subject(s) of this request.

I am making enquiries, which are concerned with

*(A) The prevention or detection of crime
*(B) The apprehension or prosecution of offenders

1. Please supply the following information concerning:

Name:	Date of birth:
Information required:	

2. The information is necessary for investigating the offence of

3. Please supply reasons why this information is necessary (if this section is left blank due to the sensitivity of the investigation, the form requires the authorisation of a superintendent or higher).

I can verify that the personal data requested is required for the reason given above, and that failure to disclose the data would be likely to prejudice these matters.

I confirm that to the best of my knowledge the information supplied herewith is complete and accurate.

4. Signed: Rank:
Name: (BLOCK CAPITALS) Date:

5. Authorising Signature: Rank:
Name: (BLOCK CAPITALS) Date:
This application must be authorised by an Inspector or above)

* Please delete as appropriate

THIS FORM MUST BE ATTACHED TO THE CASE PAPERS AND RETAINED FOR A MINIMUM OF FIVE YEARS IN LINE WITH CURRENT FORCE POLICY.

Heart of England NHS
NHS Foundation Trust

Attachment 4: Equality and Diversity - Policy Screening Checklist

Policy/Service Title: Confidentiality policy	**Directorate: Corporate Affairs**
Name of person/s auditing/developing/authoring a policy/service: Fateha Choudhury	
Aims/Objectives of policy/service:	

Policy Content:

- For each of the following check the policy/service is sensitive to people of different age, ethnicity, gender, disability, religion or belief, and sexual orientation?
- The checklists below will help you to see any strengths and/or highlight improvements required to ensure that the policy/service is compliant with equality legislation.

1. Check for DIRECT discrimination against any group of SERVICE USERS:

Question: Does your policy/service contain any statements/functions which may exclude people from using the services who otherwise meet the criteria under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
1.1	Age?		**X**		**X**		**X**
1.2	Gender (Male, Female and Transsexual)?		**X**		**X**		**X**
1.3	Disability?		**X**		**X**		**X**
1.4	Race or Ethnicity?		**X**		**X**		**X**
1.5	Religious, Spiritual belief (including other belief)?		**X**		**X**		**X**
1.6	Sexual Orientation?		**X**		**X**		**X**
1.7	Human Rights: Freedom of Information/Data Protection		**X**		**X**		**X**

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

2. Check for INDIRECT discrimination against any group of SERVICE USERS:

Question: Does your policy/service contain any statements/functions which may exclude employees from operating the under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
2.1	Age?		**X**		**X**		**X**
2.2	Gender (Male, Female and Transsexual)?		**X**		**X**		**X**
2.3	Disability?		**X**		**X**		**X**
2.4	Race or Ethnicity?		**X**		**X**		**X**
2.5	Religious, Spiritual belief (including other belief)?		**X**		**X**		**X**
2.6	Sexual Orientation?		**X**		**X**		**X**

2.7	Human Rights: Freedom of Information/Data Protection		**X**		**X**		**X**

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING DIRECT DISCRIMINATION = 0

3. Check for DIRECT discrimination against any group relating to EMPLOYEES:

Question: Does your policy/service contain any conditions or requirements which are applied equally to everyone, but disadvantage particular persons' because they cannot comply due to:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
3.1	Age?		**X**		**X**		**X**
3.2	Gender (Male, Female and Transsexual)?		**X**		**X**		**X**
3.3	Disability?		**X**		**X**		**X**
3.4	Race or Ethnicity?		**X**		**X**		**X**
3.5	Religious, Spiritual belief (including other belief)?		**X**		**X**		**X**
3.6	Sexual Orientation?		**X**		**X**		**X**
3.7	Human Rights: Freedom of Information/Data Protection		**X**		**X**		**X**

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

4. Check for INDIRECT discrimination against any group relating to EMPLOYEES:

Question: Does your policy/service contain any statements which may exclude employees from operating the under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
4.1	Age?		**X**		**X**		**X**
4.2	Gender (Male, Female and Transsexual)?		**X**		**X**		**X**
4.3	Disability?		**X**		**X**		**X**
4.4	Race or Ethnicity?		**X**		**X**		**X**
4.5	Religious, Spiritual belief (including other belief)?		**X**		**X**		**X**
4.6	Sexual Orientation?		**X**		**X**		**X**
4.7	Human Rights: Freedom of Information/Data Protection		**X**		**X**		**X**

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING INDIRECT DISCRIMINATION = 0

Signatures of authors: **Date of signing:**

When completed please return this action plan to the Trust Equality and Diversity Lead; Pamela Chandler or Jane Turvey. The plan will form part of the quarterly Governance Performance Reviews

Attachment 5: Consultation and Ratification Checklist

Title	Confidentiality Policy V5.2

	Ratification checklist	Details
1	Is this a: **Combined Policy & Procedure**	
2	Is this: **Revised**	
3*	Format matches Policies and Procedures Template (Organisation-wide)	yes
4*	Consultation with range of internal /external groups/ individuals	Not applicable, minor changes
5*	Equality Impact Assessment completed	yes
6	Are there any governance or risk implications? (e.g. patient safety, clinical effectiveness, compliance with or deviation from National guidance or legislation etc)	no
7	Are there any operational implications?	no
8	Are there any educational or training implications?	no
9	Are there any clinical implications?	no
10	Are there any nursing implications?	no
11	Does the document have financial implications?	no
12	Does the document have HR implications?	no
13*	Is there a launch/communication/implementation plan within the document?	Not applicable, minor changes
14*	Is there a monitoring plan within the document?	yes
15*	Does the document have a review date in line with the Policies and Procedures Framework?	yes
16*	Is there a named Director responsible for review of the document?	yes
17*	Is there a named committee with clearly stated responsibility for approval monitoring and review of the document?	yes

Document Author / Sponsor	**Ratified** by (Chair of Trust Committee or Executive Lead)
Signed – Fateha Choudhury	**Signed** - Lisa Thomson
Title – Information Governance Manager	**Title** - Director of Corporate Affairs
Date –	**Date** –