Mersey Care NHS
NHS Foundation Trust

| | |
|---|---|
| **Policy Number** | IT04 |
| **Policy Name** | Corporate Records |
| **Policy Type** | Trust-wide Non-Clinical |
| **Accountable Director** | Director of Informatics and Performance Improvement |
| **Author** | Information Governance Manager |
| **Recommending Committee** | Joint Senior Information Risk Owner / Caldicott Sub Committee |
| **Approving Committee** | Acquisition Steering Group |
| **Date Originally Approved** | February 2016( Review July 2016) |
| **Next Review Date** | February 2018 |

This document is a valid document, however due to organisation change some references to organisations, organisational structures and roles have now been superseded. The table below provides a list of the terminology used in this document and what it has been replaced with. When reading this document please take account of the terminology changes on this front cover

| Terminology used in this Document | New terminology when reading this Document |
|---|---|
| Mersey Care NHS Trust | Mersey Care NHS Foundation Trust |
| Executive Director of Finance | Director of Informatics and Performance Improvement |
| Information Governance Committee or Information Governance and Caldicott Committee | Joint Senior Information Risk Owner / Caldicott Sub Committee |
| | |
| | |

Mersey Care NHS Trust

## TRUST-WIDE SERVICE BASED POLICY

# CORPORATE RECORDS

| | |
|---|---|
| **Policy Number:** | **IT04** |
| **Scope of this Document:** | **All Staff** |
| **Recommending Committee:** | **Joint SIRO and Information Governance Committee** |
| **Approving Committee:** | **Executive Committee** |
| **Date Ratified:** | **February 2016** |
| **Next Review Date (by):** | **February 2018** |
| **Version Number:** | **2016 – Version 3** |
| **Lead Executive Director:** | **Executive Director of Finance** |
| **Lead Author(s):** | **Information Governance Manager** |

## TRUST-WIDE CLINICAL SERVICE BASED POLICY

**2016 – Version 3**

**Quality, recovery and wellbeing at the heart of everything we do**

Mersey Care NHS Trust

# TRUST-WIDE SERVICE BASED POLICY

# CORPORATE RECORDS

## Further information about this document:

| | |
|---|---|
| Document name | **IT04 – Corporate Records** |
| Document summary | **This policy defines the framework to ensure the Trust meets its obligations in relation of Information Governance and Records Management. This policy is issued as guidance on the creation, storage and management of Corporate Records.** |
| Author(s)<br><br>Contact(s) for further information about this document | **Linda Yell**<br>**Information Governance Manager**<br>**Telephone: 0151 471 2686**<br>**Eail: linda.yell@merseycare.nhs.uk** |
| Published by<br><br>Copies of this document are available from the Author(s) and via the trust's website | **Mersey Care NHS Trust**<br>**V7 Building**<br>**King Business Park**<br>**Prescot**<br>**Liverpool**<br>**L34 1PJ**<br>**Your Space Extranet: http://nww.portal.merseycare.nhs.uk**<br>**Trust's Website www.merseycare.nhs.uk** |
| To be read in conjunction with | **IT02 – IM&T Security Policy**<br>**IT12 – Information Governance Policy**<br>**IT13 – Freedom of Information Policy**<br>**IT14 – Data Protection Act Policy** |
| **This document can be made available in a range of alternative formats including various languages, large print and braille etc** | |
|  | |

## Version Control:

| | | Version History: |
|---|---|---|
| Version 3 | Information Governance Committee, Executive Director of Finance, Corporate Document Review Group (Feb 16), Executive Committee (Mar 16) | 2016 |

**SUPPORTING STATEMENTS** – this document should be read in conjunction with the following statements:

## SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

## EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

## CONTENTS

# 1. EXECUTIVE SUMMARY

This policy defines the framework to ensure the Trust meets its obligations in relation to Information Governance and Records Management.

Implementation of and adherence to this policy will ensure:

- Corporate Records and Information are held, used and obtained in accordance with the Data Protection Act 1998 and Freedom of Information Act 2000.
- Corporate Records are safeguarded against the risk of data breach, loss, damage, destruction.
- Corporate Records are stored in accordance with the NHS Code of Records Management.
- Staff are aware of their responsibilities in respect of Records Management and Information Governance.
- This policy is applicable to all staff working for, or with, Mersey Care NHS Trust

This policy should be read in conjunction with the following Trust policies:-

- IM&T Security Policy
- Information Governance Policy
- Data Protection Act Policy
- Freedom of Information Policy

# 2 INTRODUCTION

## 2.1 RATIONALE

The term `corporate records' means all other records held in the Trust which are not health records. The public have a right to access corporate records and information, subject to certain exemptions, under the Freedom of Information Act. This came into force on 1st January 2005. Departments who receive requests must pass them onto the Communications Team without delay as the Trust has 20 working days in which to respond. The Trust Communications Team will co-ordinate a response with final sign off by the Senior Information Risk Owner. See Trust Freedom Of Information Policy for further information.

. 

## 2.2 SCOPE

This policy applies to all staff who create any corporate record within the organisation. This policy covers all aspects of information use within the organisation, including but not limited to:-

- Personnel information/human resources
- Organisational Information

- Estates/Engineering
- Financial
- IM&T
- Purchasing / supplies

The policy covers all aspects of processing information in relation to:-

- Structured record systems-paper and electronic

### 2.3 PRINCIPLES

Corporate Records Management ensures that one of the Trusts most important assets, information, is respected and held in secure and manageable conditions and the Trust can comply with its Records Management duties to comply with current legislation. It is therefore of paramount importance to ensure that corporate records and the information they contain are efficiently managed on the basis of the HORUS categorization:

- Held safely and confidentially
- Obtained fairly and effectively
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

## 3 POLICY

### 3. 1 Electronic corporate records

Corporate information refers to information generated by an organisation other than clinical (or service user) information. The term describes the records generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the Trust:

Electronic corporate records must be accessible and retrievable when and where required. It is **NOT** only concerned with corporate records that are part of a formal electronic document and record management system (EDRMS), but includes records on network drives and in shared folders. Emails and attachments, and web pages on Internet and Intranet sites that are considered corporate records. When handling any type of record, it is important to make the distinction between a record and a document. A document becomes a record when it has been finalised and become part of an organisation's corporate information. At this point, the record should not be amended and should only be held in the corporate system, e.g. the network drive, shared folder or EDRMS, and not on a local drive on a PC or laptop. Due to the nature of electronic documents, it is vital that a process of version control is in place, so that changes are recognisable and taken into account during any decision making process.

Electronic records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle, including their migration across systems.

Ideally, the electronic record systems in place should:

- Provide audit trails to accurately log when records are created, accessed or disposed of;
- Have a logical filing structure to enable the quick and efficient filing and retrieval of records when required and enable implementation of authorised disposal arrangements, i.e. archiving, migration to another format or destruction;
- Control access to records through a variety of security measures,
  including user verification, password protection and access monitoring where appropriate;
- Support technological upgrades to ensure records remain accessible and usable throughout their life cycle;
- Permit cross-referencing of electronic records to their paper counterparts (where dual systems are maintained).

All final documents must be Trust branded and be on corporate templates, please see Trust Policy on Policy Development.

### 3.2 Referencing

The referencing system should meet the business needs, and be easily understood by staff members that create electronic documents and records.

Several types of referencing can be used, e.g:-alphanumeric; alphabetical; numeric; keyword.

The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

### 3.3 Naming

Also known as file naming conventions, the National Archives offers the following advice:

- Give a unique name to each record;
- Give a meaningful name which closely reflects the records contents;
- Express elements of the name in a structured and predictable order;

- Locate the most specific information at the beginning of the name and the most general at the end;
- Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

### 3.4 Filing structure

Clear and logical filing structures that aid retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing. Filing of corporate records to local drives on PCs and laptops is strongly discouraged.

## 4. Paper corporate records

### 4.1 Filing structure

Clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing.

Robust tracking / tracing processes must be in place, which enable the movement and location of records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, e.g. a book that staff members sign when a corporate record is removed or returned might be appropriate. A document becomes a record when it has been finalised and become part of an organisation's corporate information. With paper records, a further distinction must be made between the original record and a copy of that record.

The original record should only be held in the corporate recordkeeping system, and not in staff desk drawers, etc. Ideally, a paper record-keeping system should ensure that:

- Logs are kept to accurately document when records are created (i.e. the date that a document becomes a formal corporate record), accessed (e.g. a sign-out book) and disposed of;
- Records are grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. archiving or destruction;
- Suitable storage areas are used to ensure records remain accessible and usable throughout their life cycle;
- Access to records is controlled through a variety of security measures, e.g. authorised access to storage and filing areas, lockable storage areas;
- Issue from and return to storage areas on site or to authorised off-site facilities is documented.

### 4.2 Referencing

Referencing systems should meet the business needs, and be easily understood by staff members that create, file or retrieve paper records. Several types of referencing can be used, e.g. alphanumeric; alphabetical; numeric; keyword. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, e.g. ES for Estates, followed by a unique number for each record created by the Estates function. It may be more feasible in some circumstances to give a unique reference to the file in which the record is kept and identify the record by reference to date and format.

### 4.3 Naming

Also referred to as file naming conventions. The National Archives offers the following advice:

- Give a unique name to each record;
- Give a meaningful name which closely reflects the record contents;
- Express elements of the name in a structured and predictable order;
- Locate the most specific information at the beginning of the name and the most general at the end;
- Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

### 4.4 Indexing and filing

The index (or register) is primarily a signpost to where paper corporate records are stored, e.g. the relevant folder or file. However, it can also be a guide to the information contained in those records. The index should be arranged in a user-friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear and logical names to assist filing and retrieval of records. Filing of corporate records in desk drawers should not happen.

## 5. Classification marking guidance (Department of Health)

This NHS Information Governance (IG) guidance is provided as good practice for NHS organisations of all types to consider in marking the records for which they are responsible. It is applicable to both information recorded on paper and that processed electronically including printouts, reports etc. Through the application of this guidance, NHS organisations should be able to further demonstrate the effectiveness of their local IG practices. This guidance should be considered alongside other published NHS IG Codes of Practice and guidance for Confidentiality, Records Management, Information Security Management, Legal and Professional obligations. These are currently available for download through the Department of Health website at www.dh.gov.uk.

### 5.1 Introduction

There has previously been no single or consistent system of

classification marking of information within the NHS. Many NHS bodies have adopted their own classification schemes and this can cause confusion when organisations merge or where information is shared between organisations. This is particularly marked where, as in the case of, for example, NHS and Social Care organisations, there may be a need for common assurances in information partnerships. There is also danger of a lack of consistency in data handling and retention practice when information is shared with non-NHS bodies that relate to several NHS organisations. The lack of a single coherent system also hampers the development of appropriate IT system protocols for the NHS.

### 5.2 Background and classification scheme outline

This guidance paper sets out a proposed simple scheme of classification relevant to the needs of NHS organisations and for the common benefit of all. It is similar to that used in central Government and other public sector organisations but takes account of important differences in the nature of NHS business activity and the kind of information used between the NHS and other public sector environments. Equally, the NHS does not have a requirement for the full range of protective markings used in Government. For example, central Government uses six categories of information classification, two of which - Secret and Top Secret - are, usually, only relevant to a very limited number of very serious situations involving national security and economic stability. The others are Confidential, Restricted, Protect and Unclassified. These are more relevant within an NHS context and are terms that were considered in developing this classification guidance. Categories proposed for
use are prefixed "**NHS**" to indicate their relevance to a particular environment. NHS information that has no classification requirement should be considered **Unclassified** and may optionally be marked as such.

### 5.3 NHS Confidential

In Government, the marking "Confidential" would, for example, denote information that could undermine the viability of national organisations, damage security operations or national finances or economic and commercial interests. These considerations are unlikely to apply in an NHS context. But within the NHS it is generally recognised, and there is a substantial body of case law that requires, that person-identifiable clinical information should always be held confidentially (*Confidentiality*: NHS Code of Practice). Therefore, the marking **NHS CONFIDENTIAL** should be used for that kind of information (e.g. patients' clinical records, patient identifiable clinical information, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies). This will include patient demographic details that might identify people who have had a GP contact/hospital appointment within a particular timeframe or who may have a particular condition. (**NOTE**: In order to safeguard confidentiality, the term "NHS Confidential" should **never** be used on correspondence to a patient.)

The endorsement **NHS CONFIDENTIAL** should be included at the top centre of every page of the document. Documents so marked should be held securely at all times. That is, they should be stored in a locked room or equivalently within secured electronic systems to which only authorised persons have access. They should not be unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed containers and not unattended at any stage. Documents marked NHS CONFIDENTIAL not in a safe store or transport should be kept out of sight of visitors or others not authorised to view them.

### 5.4 Other uses of NHS Confidential

The endorsement **NHS CONFIDENTIAL** should also be used to mark all other sensitive information. That is, material the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or it's officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

A paper, printout or report etc marked **NHS CONFIDENTIAL** may also be endorsed with a suitable descriptor indicating the reason for the classification e.g. 'NHS CONFIDENTIAL – PATIENT INFORMATION' or 'NHS CONFIDENTIAL – COMMERCIAL'.
A list of the relevant descriptors is included in **Table 1**. The endorsement should be included at the top centre on every page of the document. **NHS CONFIDENTIAL** documents should be stored in lockable cabinets or equivalently secured electronic systems. Information may be classified **NHS CONFIDENTIAL** in the light of the circumstances at a particular time. The classification should be kept under review and the information de-classified when the need for this protection no longer applies. NHS use of an equivalent classification for "Restricted" is unnecessary when **NHS CONFIDENTIAL** is used.

### 5.5 NHS Protect

In Government a new marking of **"**PROTECT" was recently introduced.

This discretional marking may be used in order to avoid unauthorised access to information. It establishes basic principles to handle with care, take relevant precautions and dispose of properly. In the NHS context, it is therefore possible for NHS organisations to adopt and use an equivalent **NHS PROTECT** marking, with or without descriptors, for information that requires protection below that of **NHS CONFIDENTIAL** and where care in handling is still necessary. NHS organisations that choose to adopt **NHS PROTECT** must therefore ensure their staff and business partners are aware of the different expectations and arrangements that apply for the protection and assurance of **NHS CONFIDENTIAL** and **NHS PROTECT** marked information.

### 5.6 Freedom of Information

When classifying NHS documents regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to an inappropriate decision not to disclose information that would later be embarrassing to the organisation (for example, where there was an appeal against non-disclosure or the Information Commissioner became involved). Protective markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemption – See 4.7 Table 2. Further information about the Act and its exemptions (including the drafts of documents that are intended for publication application of the "public interest" test) is available on the website of the Information Commissioner (www.informationcommissioner.gov.uk) Also see the Trust Freedom of Information Act Policy

### 5.7 Classification of NHS Information - Marking Guidance for NHS Organisations

**NHS CONFIDENTIAL** - appropriate to paper and electronic documents and files containing person identifiable **clinical** or NHS **staff** information and **other sensitive** information.

**NHS PROTECT** – Discretionary marking that may be used for information classified below NHS Confidential but requiring care in handling. Descriptors may also be used as required.

**Table 1 – Descriptors that may be used with "NHS CONFIDENTIAL" or "NHS PROTECT" marking**

**Category Definition**

- Appointments Concerning actual or potential appointments not yet announced.
- Barred - Where there is a statutory (Act of Parliament or European Law) prohibition on disclosure or disclosure would constitute a contempt of Court (information the subject of a court order).
- Board - Documents for consideration by an organisation's Board

of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way).
- Commercial Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
- Contracts Concerning tenders under consideration and the terms of tenders accepted.
- For Publication Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
- Management Concerning policy and planning affecting the interests of groups of staff. (Note: Likely to be exempt only in respect of some health and safety issues).
- Patient Information Concerning identifiable information about patients
- Personal Concerning matters personal to the sender and/or recipient.
- Policy Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).
- Proceedings The information is (or may become) the subject of, or concerned in a legal action or investigation.
- Staff Concerning identifiable information about staff.

**Table 2 - Freedom of information act exemptions**

Category Possible Exemption [section(s) of the FOI Act]

- Appointments S 40 Personal information (may be subject to a public interest test)
- Barred S 44 Legal prohibitions on disclosure Board
- Commercial S 43 Commercial interests (subject to a public interest test)
- Contracts S 43 Commercial interests (public interest test)
- For Publication S 22 For future publication (public interest test)
- Management S 38 Endanger health and safety (public interest test)
- Personal S 40 Personal Information (may be subject to public interest test)
- Policy S 22 For future publication (public interest test)
- Proceedings S 30 Investigations and proceedings
- S 31 Law enforcement

## 6. Retention periods

Part 2 of the NHS Records Management Code of Practice contains retention periods for both health and corporate records. Records, both paper and electronic, should not be kept for longer than necessary. For a copy of the full document, contact the Trust Information Governance Manager.

## 7. Subject access requests for corporate records

Under the Data Protection Act 1998 individuals have a right to make a request in writing for a copy of the information held about them on computer and in some manual filing systems. This is called a subject access request. For guidance on Subject access requests please see the Trust Confidentiality and Data Sharing Policy and Data Protection Act Policy.

### 7.1 Is this a subject access request?

Determine whether the person's request is a subject access request. Any written enquiry that asks for information you hold about the person making the request (data subject) can be construed as a subject access request. Any requests for access must be in writing. The written request must contain sufficient information to enable the Trust to conduct the search required e.g. Name, Address and Date of Birth. Compliance with the request is not obligatory until the Trust has been provided with adequate information and identity validation. Check with the relevant department manager that the information is not normally released as part of normal business processes. If it is releasable as part of normal business processes refer to the relevant department manager who should deal with the request. Please see The Trust Freedom Of Information Act Policy, Data Protection Act Policy and Trust Confidentiality and Data Sharing Policy for further guidance.

## 8. MONITORING & REVIEW

Monitoring and review of this Policy will take place by areas identified by the Information Governance Committee undertaking an annual audit of Corporate Records. The Information Governance Committee will receive an annual report in respect of the audit findings. The Information Governance Committee will make recommendations in respect of the management of records and instigate an action plan as required.

## 9. DEVELOPMENT & CONSULTATION PROCESS

This policy has been developed by the Information Governance Manager. The policy has also been reviewed by the Caldicott Guardian, Senior Information Risk Owner and Information Governance Committee.

## 10. DUTIES & RESPONSIBILITES

**Chief Executive**

The Chief Executive as the accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms

are in place to comply with Information Governance and Records Management.

**Senior Information Risk Owner**
The Trust's Senior Information Risk Owner has a particular responsibility in ensuring that a robust framework to comply with the retention of records complies with all legislation across the Trust and that members of staff within the Trust comply with all requirements of Information Governance, which is driven by various legislation and guidelines issued by the Department of Health, Health & Social Care Information Centre and other sources.

**Information Governance Manager & Information Governance Committee**
The Information Governance Manager is responsible for ensuring that the Trust is working within the legal framework of the Data Protection Act, Freedom of Information Act, NHS Code of Practice for Records Management, NHS Code of Practice for Confidentiality, Information Governance Standards. The Information Governance Manager is the designated trust representative that liaises with the Information Commissioners Office and conducts internal reviews for any Freedom of Information Act complaints. The Information Governance and Caldicott Committee ensures the Trust operates within the Information Governance framework and reports to the Trust Executive Committee.

**Senior Managers**
It is the responsibility for all Senior Managers to ensure that staff work within the boundaries of the Trust policies and procedures and are aware of their responsibilities.

**All staff**
All employees of the Trust, or staff working in a voluntary capacity, agency or independent contractors must adhere to the current legislative framework and Trust policies.

## 11 REFERENCE DOCUMENTS

Freedom of Information Act 2000
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/2000/cukpga_20000036_en_1
Data Protection Act 1998
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1998/cukpga_19980029_en_1
Code of practice on the discharge of public authorities' functions underPart 1 of the Freedom of Information Act 2000 – dealing with requests for information.
http://www.foi.gov.uk/reference/imprep/codepafunc.htm
Code of practice on the management of records Issued under section 46 of the Freedom of Information Act 2000
http://www.foi.gov.uk/reference/imprep/codemanrec.htm

Trust Confidentiality Code and Data Sharing Policy
Trust Data Protection Act Policy
Trust IM&T Security Policy

## 12. BIBLIOGRAPHY

No Bibliography

## 13. GLOSSARY

No Glossary

## 14. APPENDIX

No appendices

# Equality and Human Rights Analysis

| |
|---|
| **Title:**<br>Corporate Records Policies |
| **Area covered: Trustwide** |

| |
|---|
| **What are the intended outcomes of this work?** *Include outline of objectives and function aims*<br>To give guidance on the creation, storage and management of Corporate Records to ensure the Trust meets its obligations in relation to Information Governance and Records Management. |
| **Who will be affected?** *e.g. staff, patients, service users etc*<br>Staff |

| **Evidence** |
|---|
| **What evidence have you considered?** |
| **Disability (including learning disability)** |
| **Sex** |
| **Race** *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.* |
| **Age** *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.* |
| **Gender reassignment (including transgender)** *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.* |
| **Sexual orientation** *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.* |
| **Religion or belief** *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.* |
| **Pregnancy and maternity** *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.* |
| **Carers** *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.* |
| **Other identified groups** *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.* |

| **Cross Cutting** *implications to more than 1 protected characteristic* |
|---|
| |

| **Human Rights** | **Is there an impact?**<br>**How this right could be protected?** |
|---|---|
| **Right to life (Article 2)** | *Use not engaged if Not applicable* |
| **Right of freedom from inhuman**<br>**and degrading treatment (Article 3)** | *Use supportive of a HRBA if applicable* |
| **Right to liberty (Article 5)** | |
| **Right to a fair trial (Article 6)** | |
| **Right to private and family life**<br>**(Article 8)** | |
| **Right of freedom of religion or belief**<br>**(Article 9)** | |
| **Right to freedom of expression**<br>**Note: this does not include insulting language such as racism (Article 10)** | |
| **Right freedom from discrimination**<br>**(Article 14)** | |

| Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.* |
|---|
| |
| |
| |

## Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010*

### Eliminate discrimination, harassment and victimisation

### Advance equality of opportunity

### Promote good relations between groups

### What is the overall impact?

### Addressing the impact on equalities

*There needs to be greater consideration re health inequalities and the impact of* each individual development /change in relation to the protected characteristics and vulnerable groups

## Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.*

## For the record

**Name of persons who carried out this assessment:**
**Kate Greenwood** **Gina Kelly reviewed document – no changes required**
**Jacquie Ruddick**
**Gina Kelly**

**Date assessment completed:**
19 October 2011 **Reviewed 20 January 2016**

**Name of responsible Director:**
Jim Hughes

| **Date assessment was signed:** |
| --- |
| 19/10/2011 |

# Action plan template

This part of the template is to help you develop your action plan. You might want to change the categories in the first column to reflect the actions needed for your policy.

| Category | Actions | Target date | Person responsible and their area of responsibility |
|---|---|---|---|
| **Monitoring** | | | |
| **Engagement** | | | |
| **Increasing accessibility** | | | |

| IMPLEMENTATION PLAN | Issues identified / Action to be taken | Time-Scale |
|---|---|---|

| IMPLEMENTATION PLAN | Issues identified / Action to be taken | Time-Scale |
|---|---|---|
| **Co-ordination of implementation**<br>• How will the implementation plan be co-ordinated and by whom?<br>*Clear co-ordination is essential to monitor and sustain progress against the implementation plan and resolve any further issues that may arise.* | • The implementation plan will be co-ordinated by the e.Governance Manager. The plan will include distribution of the policy in accordance with the guidance in Policy and Procedure for the Development, Ratification, Distribution and Reviewing Policies and Procedures. | Jan 2013 |
| **Engaging staff**<br>• Who is affected directly or indirectly by the policy?<br>• Are the most influential staff involved in the implementation?<br>*Engaging staff and developing strong working relationships will provide a solid foundation for changes to be made.* | • This policy is applicable to all staff working for, or with, Mersey Care NHS Trust (the trust). | |
| **Involving service users and carers**<br>• Is there a need to provide information to service users and carers regarding this policy?<br>• Are there service users, carers, representatives or local organisations who could contribute to the implementation?<br>*Involving service users and carers will ensure that any actions taken are in the best interest of services users and carers and that they are better informed about their care.* | • There is no need to provide service users or carers a copy of this Policy however it will be available via the Trust website or copies will be provided upon request in different formats.<br>• Service Users and Carers will not be involved in implementing the procedure. | |

| IMPLEMENTATION PLAN | Issues identified / Action to be taken | Time-Scale |
|---|---|---|
| **Communicating**<br>• What are the key messages to communicate to the different stakeholders?<br>• How will these messages be communicated?<br>*Effective communication will ensure that all those affected by the policy are kept informed thus smoothing the way for any changes. Promoting achievements can also provide encouragement to those involved.* | • Key messages are:<br>- That all staff must comply with current legislation outlined within the Data Protection Act 1998, Freedom of Information Act and NHS Code of Practice for Records Management.<br>• All staff will be able to access the policy via their manager or the Trust website. | |
| **Training**<br>• What are the training needs related to this policy?<br>• Are people available with the skills to deliver the training?<br>*All stakeholders need time to reflect on what the policy means to their current practice and key groups may need specific training to be able to deliver the policy.* | • Completion of Induction and Corporate Mandatory Training.<br>• Management & retention of Records to comply with NHS Code of Practice for Records Management | |
| **Resources**<br>• Have the financial impacts of any changes been established?<br>• Is it possible to set up processes to re-invest any savings?<br>• Are other resources required to enable the implementation of the policy eg. increased staffing, new documentation?<br>*Identification of resource impacts is essential at the start of the process to ensure action can be taken to addess issues which may arise at a later stage.* | • There are no additional financial implications arising from the implementation of this procedure. | |

| IMPLEMENTATION PLAN | Issues identified / Action to be taken | Time-Scale |
|---|---|---|
| **Securing and sustaining change**<br>• Have the likely barriers to change and realistic ways to overcome them been identified?<br>• Who needs to change and how do you plan to approach them?<br>• Have arrangements been made with service managers to enable staff to attend briefing and training sessions?<br>• Are arrangements in place to ensure the induction of new staff reflects the policy?<br>*Initial barriers to implementation need to be addressed as well as those that may affect the on-going success of the policy* | • Consideration of potential barriers was discussed during the development of the procedure. | |
| **Evaluating**<br>• What are the main changes in practice that should be seen from the policy?<br>• How might these changes be evaluated?<br>• How will lessons learnt from the implementation of this policy be fed back into the organisation?<br>*Evaluating and demonstrating the benefits of new policy is essential to promote the achievements of those involved and justifying changes that have been made.* | • Increased awareness in respect of the NHS Code of Practice for Records Managment and staff's responsibilities to comply with Data Protection Act and Freedom of Information Act.<br>• Audits will also be conducted with Corporate areas to monitor retention & destruction of records and comply with current legislation.<br>• The outcome of audit reports will be reported by the Information Governance Manager to the Information Governance Committee. | March annually |
| <u>Other considerations</u> | | |