Mersey Care NHS
NHS Foundation Trust

Policy Number	IT14
Policy Name	Data Protection Act Policy
Policy Type	Trust-wide Non clinical
Accountable Director	Director of Informatics and Performance Improvement
Author	Director of Informatics and Performance Improvement
Recommending Committee	Joint Senior information Risk Owner / Caldecott Committee
Approving Committee	Acquisition Steering Group
Date Originally Approved	December 2015 (reviewed July 2016)
Next Review Date	December 2017

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however due to organisation change some references to organisations, organisational structures and roles have now been superseded.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 and Caldicott Committee **or** Information Governance Committee **or** Joint SIRO and Information Governance Committee.	Joint Senior Information Risk Owner / Caldicott Committee
Trust Board	Board of Directors

Mersey Care NHS Trust

TRUST-WIDE SERVICE BASED POLICY

DATA PROTECTION ACT POLICY

Policy Number:	**IT14**
Scope of this Document:	**All Staff**
Recommending Committee:	**Information Governance & Caldicott Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**December 2015**
Next Review Date (by):	**December 2017**
Version Number:	**July 2015 – Version 3** (For Ratification)
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Information Governance Manager**

TRUST-WIDE SERVICE BASED POLICY

July 2015 – Version 3

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

Mersey Care NHS Trust

TRUST-WIDE SERVICE BASED POLICY

DATA PROTECTION ACT POLICY

Further information about this document:

Document name	**Corporate Data Protection Act Policy IT14**
Document summary	This Policy is issued as a framework to everyone working with Personal Identifiable Information (also known as Personal Confidential information) regardless of what media it is retained in. This policy outlines current legislation detailed in the Data Protection Act 1998 and sets out the Trust's and employees' responsibilities. This document is presented in a standard structure and format. It will be made available in appropriate, alternative languages and formats on request.
Author(s) Contact(s) for further information about this document	**Linda Yell,** **Information Governance Manager** **Telephone: 0151 471 2686** **Email: linda.yell@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **8 Princes Parade** **Princes Dock** **St Nicholas Place** **Liverpool** **L3 1DL** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT02** IM&T Security Policy **IT10** Confidentiality and Information Sharing Policy **IT13** Freedom of Information Act Policy **IT12** Information Governance & Information Risk 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	July 2015

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 Page

EXECUTIVE SUMMARY

This policy defines the framework to ensure the Trust meets its obligations in relation to the Data Protection Act 1998.

Implementation of and adherence to this policy will ensure:

- Information is held, used and obtained in accordance with the Data Protection Act 1998
- The Trust manages the process of Subject Access and provides the right of access to individuals which covers service users, employees any other individual about whom the Trust holds personal data.
- Any disclosure of confidential information is lawful.
- Staff are trained and aware of their responsibilities in respect of the Data Protection Act 1998,
- This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust.

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

- IM&T Security Policy
- Confidentiality and Information Sharing Policy
- Freedom of Information Act Policy
- Information Governance & Information Risk Policy

1. INTRODUCTION

1.1 Rationale

Mersey Care NHS Foundation Trust acknowledges the importance of good practice regarding personal information and endorses the principles of data protection. In addition, this policy outlines the general managerial policy and approach to meeting good practice.

The Data Protection Act 1998 came into force on 1st March 2000. The Act entitles a living individual, with certain exceptions, to view or be provided with a copy of information held in relation to the individual. The Act covers manually or electronically recorded data and the individual is entitled to know the purposes for which it is being processed. A request for this data under the Act is commonly known as a Subject Access Request.

The Data Protection Act 1998 only applies to information held about living individuals. Provision for requests for access to records relating to the deceased is provided under the Access to Records Act 1990.

1.2 Scope

This Policy will apply to all Trust employees, bank staff, agency staff, volunteers, Independent Contractors and Non-Executive Directors. A failure to adhere to this Policy and its associated procedures may result in disciplinary action. Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of and adhere to this Policy. They are also responsible for ensuring staff are updated in regard to any changes in this Policy.

This policy endorses and complies with the Health and Social Care Information Centre's Code of Practice on Confidential Information, the Caldicott Reviews of the Uses of Patient-Identifiable Information (1997) and Information Governance (2013) and the Information Commissioners Office Subject Access Code of Practice, which cover the use and disclosure of patient information.

- It will provide a framework within which the Trust will ensure compliance with the requirements of the Act
- It will underpin any operational procedures and activities connected with the implementation of the Act
- This policy is supported by the Trust Data Protection Guidelines and Procedures

All personal data whether it is held manually or on computers, is subject to the requirements of the Data Protection Act. This Act sets out the standards that must be satisfied when obtaining, recording, holding, using or disposing of personal data.

1.3 Principles

The Trust needs to collect and use certain types of information about people with whom it deals in order to operate. This includes 'personal data' as defined by the Data Protection Act

In practice the vast majority of information held by the Trust about individuals will be 'personal data' and subject to the requirements of the Act. This includes information about current, past and prospective employees, suppliers, patients, and others with whom it communicates.

In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments for business data, for example.

This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998. The Trust must comply with the Act. The Trust regards the lawful and correct treatment of personal information as very important to providing services and to maintaining confidence between partnership organisations. The Trust ensures that personal information fully endorses and adheres to the Principles of data protection, as defined in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

- shall be processed fairly and lawfully and, in
- particular, shall not be processed unless specific conditions are met;
- shall be obtained only for one or more specified and
- lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- shall be accurate and, where necessary, kept up to date;
- shall not be kept for longer than is necessary for that purpose or those purposes;
- shall be processed in accordance with the rights of data subjects under the Act;

and that:

- appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. POLICY

The Data Protection Act puts strict controls on the use of personal information, in order to enforce this, the Chief Executive has overall responsibility for compliance and is designated the data controller. The implementation of compliance is delegated to the Information Governance Manager and other designated staff.

3. IMPLEMENTATION

3.1 Trust Responsibilities

The Trust will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;

- apply strict checks to determine the length of time information is held, with reference to the NHS Code of Practice on Records Management;
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken: the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

In addition, the Trust will ensure that:

- there is a named person(s) with specific responsibility for data protection in the Trust. (Currently, the Caldicott Guardian, Information Governance Manager and Senior Information Risk Owner);
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal information is managed;
- methods of handling personal information are regularly assessed and evaluated;
- performance with handling personal information is regularly assessed and evaluated.

The Trust will ensure that confidentiality clauses are incorporated into all employee contracts of employment

All breaches of confidentiality and information security, accidental or deliberate, will be considered a serious offence and may result in a disciplinary investigation and possible dismissal.

All data loss or data breach incidents will be reviewed and monitored by the Information Governance Committee. Individual incidents will be managed in relation to assessment against the Information Commissioners Serious, Untoward Incident reporting criteria and reported as required. Individuals involved in data loss/breach incidents will be formally written to and advised of the incident and mitigating action taken by the Trust.

Please refer to the Trust policies and procedures for disclosure of information in response to Freedom of Information requests.

3.2 Definitions

The provisions of the Data Protection Act 1998 apply only to personal data. The term **'personal data'** is defined in section 1(1) as data which relate to a living individual who can be identified from those data (or from those data and other information which is in the possession of, or is likely to come into the possession of, the Trust) 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.

Data Controller – A 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. The data controller has the primary responsibility for complying with the requirements of the Act. The Trust is the data controller in respect of the vast majority of personal data that it holds (e.g. personal data about patients and staff).

Data Subject – A 'data subject' means an individual who is the subject of personal data and must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects. For example, for a medical record, the patient to whom it relates will be the data subject.

Relevant Filing System
A 'relevant filing system' is defined in section 1(1) of the Act as: Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals, in such a way that specific information relating to a particular individual is readily accessible. For example, a folder of records relating to a particular patient is a relevant filing system. If information is held in a relevant filing system is it is subject to the requirements of the Act.

Health Record – A 'health record' is defined in the Act as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a healthcare professional in connection with the care of that individual. The definition can also apply to material held on X-Ray or MRI scan. This means that when a subject access request is made, the information contained in such material must be provided to the applicant. Health records are subject to the requirements of the Act regardless of whether they are electronic or manual, how they are held or how easily they can be located.

Health Professional – A health professional is defined in the act as:

- A registered medical practitioner;
- A registered dentist as defined by section 53(1) of Dentists Act 1984;
- A registered optician as defined by section 36(1) of the Opticians Act 1989;
- A registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954 or registered person as defined by Article 2(2) of the Pharmacy (northern Ireland) Order 1976
- A registered nurse, midwife or health visitor;
- A registered osteopath as defined by section 41 of the Osteopaths Act 1993;
- A registered chiropractor as defined by section 43 of the Chiropractors Act 1994;
- Any person who is registered as a member of a professions which the Professions Supplementary to Medicine Act 1960 for the time being extends;
- A clinical psychologist, child psychotherapist or a speech therapist;
- A music therapist employed by a health service body; and
- A scientist employed by such a body as a head of department.

4. ACCESS TO PERSONAL DATA

An application to access personal data may be made by a number individuals and in a variety of circumstances:

4.1 The data subject is entitled to make a request in writing to see any personal data held about them under the Act. This is known as a Subject Access Request though there is no need for the individual to use this phrase or refer to the Act at all. Data subjects are usually asked to complete a form to ensure that the Trust has all of the information it needs in order deal with the request, but the Trust cannot insist upon this. Technically, any request in writing (e.g. letter, email, fax, social media post) sent to any Trust employee will be valid.

In exceptional circumstances, if the applicant is unable to make the application in writing, dispensation may be given for the application to be made verbally to the Trust representative who would complete the form on behalf of the applicant, but the Trust must ensure that validity of the applicant is determined before disclosure is made.

4.2 A person with written authorisation to act on behalf of the Data Subject (including solicitors, etc)

Anyone making a Subject Access Request on behalf of someone else must apply in writing together with written authorisation from the data subject, which must be signed by the data subject themselves.

A common example of such a request is where a solicitor makes a Subject Access Request on behalf of a client they are representing. A signed, written authorisation must be provided in such cases.

4.3 A Person Appointed under a Power of Attorney or by the Courts

Where a service user lacks capacity to make a Subject Access Request themselves, someone appointed to act on their behalf under a Power of Attorney (an Attorney) or by the courts (a Deputy) may submit a subject access request on behalf of the data subject. An attorney must provide proof of the Power of Attorney, which is a standard document that must have been registered with the Office of the Public Guardian before it can be used. A Deputy must provide a sealed copy of the court order appointing them as a deputy. Where in any doubt as to the validity of such documents, legal advice should be sought.

4.4 A person acting on behalf of a child

In the case of young children Subject Access Requests are likely to be exercised by those with parental responsibility for them. However, information about children is still their personal data and does not belong to anyone else, such as a parent or guardian.

The concept of *Gillick* competence, which applies in respect of medical treatment, does <u>not</u> apply to Subject Access Requests. However, the principles are similar.

Before responding to a request for information held about a child, the Trust should consider whether the child is mature enough to understand their rights under the Act. If you are confident that the child can understand their rights, then you should respond to the child rather than the

parent. If the child is unable to understand their rights under the Act, then someone with parental responsibility can make the request on their behalf.

What matters in making the above decision is whether the child is able to understand (in broad terms) what it means to make a request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

4.5 Requests for Disclosure of Service User Records in Connection with Disciplinary Hearings

Under certain circumstances managers and staff side representatives may also request disclosure of service user records for use in relation to disciplinary proceedings. In this case ***please refer to template included as Appendix 3***

4.6 The Police

There are occasions when the Trust may be asked to provide personal data to the police or another organisation that is responsible for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of taxes/duties (e.g. NHS Protect or HMRC).

In exceptional circumstances the Trust can lawfully disclose a patient's health data or other personal data in the absence of the patient's consent, without it being in breach of the DPA or the duty of confidentiality. This is the case where there is an applicable exemption under the Act, there is a public interest in disclosure being made and/or there is another legal instrument permitting or requiring disclosure (e.g. a court order or statutory power). It should never be assumed that the police or other agencies making requests have the right to obtain the information they are requesting. Such requests must be dealt with on a case-by-case basis by the Trust.

One common case is where the Trust is satisfied that the disclosure of the data is necessary for the purpose of prevention and/or detection of a crime or apprehension or prosecution of offenders. The details of this exemption are contained in **Section 29 DPA.** It is not enough to accept the police's own judgment on this. The Trust has itself to be satisfied that this ground is met. The Trust must be satisfied that non-disclosure would prejudice the police's purpose for the request.

Therefore, before disclosing any data/document to the police that may contain personal and/or confidential data, you should:

- Ascertain what specific information/documents the police want and why (in writing). Blank Section 29 DPA template request forms are held and completed by police forces and should be provided to the Trust before the disclosure.

- Consider whether it is appropriate to get the individual's consent to disclose the data/information. In some cases, this will not be appropriate (e.g. if the police are investigating a crime and seeking the patient's consent may "tip them off"). In such cases the police must explain in writing why seeking the patient's consent would in fact prejudice their investigation.

- In any case involving a patient, it is good practice to consult with the patient to obtain their consent, where possible, particularly where there may be an ongoing therapeutic relationship. The potential impact on the patient of seeking consent or making a disclosure without consent should be taken into account. Where appropriate, the views of the patient's clinician should be sought to ensure that all relevant factors are considered in deciding whether to make the disclosure.

- In cases, where it is judged to be inappropriate or impracticable to get consent then, in the absence of this, the Trust must be satisfied that it is justified to disclose. In the absence of a court order such disclosures are voluntary and it is up to the Trust, as data controller, to ensure it complies with the law. Voluntary disclosure is open to subsequent criticism, so you must only disclose patient data when it can be justified and a defence may be provided to any claim for wrongful disclosure/breach of confidence/breach of human rights – this is why the details of the initial request from the police are important and a record kept for future use.

- Any staff member, who takes the decision to disclose information, must record the fact so that there is clear evidence of the reasoning used and the circumstances of the request.

- Where in any doubt as to the lawfulness of a disclosure, the presumption should be in favour of preserving the privacy and confidence of individuals and legal advice should be sought.

4.7 Court Order (Court Directive)

In some cases the Court will make an Order for records or information to be provided either to the court or to someone else. This could be because the information is important evidence for a case being heard.

Court orders do not require consent from the data subject and must be actioned immediately. However, the Trust should ensure that the Court order is sealed and dated and contact the court should it have any doubts as to its validity.

In exceptional cases the Trust may have legitimate reasons to object to the disclosure required by the Court order (e.g. the disclosure could cause significant harm to an individual that the court may not have been aware of when making the order). In such cases the Trust must not ignore the order (this would be contempt of court) but should urgently seek legal advice in order that an application to court can be considered.

4.8 Appointed Representative of the Deceased

The Data Protection Act 1998 does not apply to information about deceased individuals. However, Health Records relating to deceased service users must be treated with the same level of confidentiality as those relating to living individuals.

Under the Access to Health Records Act 1990 a request to be provided with copies of/or view a deceased service users record can be made by the service user's personal representative or any person who may have claim arising out of the service user's death.

The personal representative (executor or next-of-kin – who may be a relative, friend or solicitor) or anyone having a claim resulting from the death has the right to apply for access to the relevant part(s) of the deceased's health record under the 'Access to Health Records Act 1990'. Where the requestor is not acting in a legal capacity, they should detail why they need access in pursuing a claim. Where they are the executor or administrator they must provide proof of appointment under the Will/Grant of probate.

4.9 Timetable for Access

For living individuals, the Data Protection Act 1998 requires Subject Access requests to be complied with within 40 days. However, under Department of Health policy, whenever possible the requests for medical records should be dealt with within 21 days.

4.10 Providing Information

When collating information for the data subject the following points should be considered:-

- Check for and ensure that any third party information has been removed or the necessary consent has been obtained from the third party;
- Check with the relevant healthcare professional for a decision to be taken in respect of whether disclosure would result in serious physical or mental harm to the data subject or any other person (see 4.9 below);
- The method of delivery should be agreed with the applicant, for example whether a meeting should take place or whether the information is copied and posted out by Recorded Special Delivery or collected in person by the applicant or sent out electronically via the Trust secure protocol.

In some circumstances information relates to both the data subject and a third party and it can be impossible to remove the third party data without removing the data subject's own personal data (e.g. a record of a service user's opinion about a relative is the personal data of both the service user and the relative).

In such circumstances the consent of the third party should be sought, where practicable. Where consent is not obtained the Trust must decide whether it is reasonable in all the circumstances to disclose the information anyway, taking into account all relevant factors including:

- any duty of confidentiality owed to the third party;
- any steps you have taken to try to get the third party individual's consent;
- whether the third party individual is capable of giving consent; and
- any stated refusal of consent by the third party individual.

4.11 Explanation of the Data
The data supplied to the applicant should be in an intelligible form and interpretation of technical terminology provided upon request. If the request has been to view records then arrangements must be made for a suitable healthcare professional/manager to be present to answer any potential questions as to the content of the record or to provide supervision.

Patients are entitled to understand who has had access to their health records. A full and meaningful audit trail, which details anyone and everyone who has accessed an individual's electronic personal confidential data, should be made available in a suitable form to patients.

4.12 Inaccuracies in Health Records
The fourth data protection principle provides that personal data shall be accurate and, where necessary kept up to date.

Any requests for alleged inaccuracies within the record to be corrected will only be made in agreement with the relevant healthcare professional in charge. If the healthcare professional agrees that the information is inaccurate the records should be updated to show that this is the case.

If the healthcare professional does not agree that the information is inaccurate, then a note recording the matters alleged to be inaccurate will be made on the record and a copy sent to the applicant. The applicant may submit an account of the inaccuracies and this will be held within the record.

When making any changes to records the continuity and auditability of the records are paramount. Therefore, where inaccurate information has been recorded in the past, the Trust must update the record to make clear that such information is now known to be inaccurate, but it may legitimately refuse to erase the inaccurate information entirely. The inaccurate information may have been relied upon by clinicians to justify their actions and the Trust may need to demonstrate this in future. For this reason, it will rarely be appropriate to completely erase information from a record, but such requests should be considered on a case by case basis.

4.13 Non-Disclosure of Information (exemptions)
There are a number of exemptions from disclosure set out under the Data Protection Act 1998. Where access is to be denied in accordance with an exemption the applicant will be informed of this.

The main exemption the Trust needs to be aware of is the exemption for health records under the Data Protection (Subject Access Modification)(Health) Order 2000. This exemption applies where disclosure is believed to be likely to cause serious harm to the physical or mental health or condition of the individual, or someone else and access would not be in accordance with the best interests or wishes of the service user. This decision would be made by the healthcare professional responsible for that individual's care.

4.14 Management and Completion of Subject Access Requests
Administrative staff processing Subject Access Request must ensure that all Subject Access Requests are lodged onto the Trust central recording databases. It must record what information has been requested, dates sent to clinicians and completion date. This will allow reports to be generated and presented to the Information Governance Committee to ensure compliance with the legislative time frames and monitoring of resources. Documentation may

also form evidence in the event of a compliant to the Trust or Information Commissioner's Office.

4.15 Fees
Mersey Care NHS Foundation Trust do not charge any fees in relation to the provision of information relating to Subject Access Requests or Access to Deceased Records.

5. DUTIES & RESPONSIBILITIES

The Information Governance Manager is responsible for:-

- Maintaining the Trust Data Protection Registration notification to the Information Commissioners Office.
- Overseeing the overall Management of Subject Access Requests process.
- Promoting Data Protection advice and awareness
- Investigating breaches of data protection and confidentiality audits
- Liaising with the Information Commissioner's Office on behalf of the Trust.

Senior Managers

- Ensuring staff whom they are responsible for are aware of and adhere to this policy.
- Ensuring staff are updated in regard to any changes in this policy.
- Ensuring that staff are aware of their obligations under the Data Protection Act 1998 and keep staff up to date with any changes of additions to the policy.

All Staff

- Must understand their legal obligation to keep personal information confidential
- Participate in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues
- Be aware of the nominated Caldicott Guardian Lead and Information Governance Lead within their Division whom they should liaise with regarding confidentiality issues.
- To challenge and verify where necessary the identity of any person who is making a request for confidential information and to determine the validity of the reason for requiring that information
- To ensure that actual or suspected breaches of the Act and/or confidentiality are reported to their line manager and via the Trust Adverse Incident Policy.
- To participate in audits/reviews of working practices to identify areas of improvement with regard to patient confidentiality and to implement any measures identified
- To ensure data is recorded accurately and in a legible Manner.

5.2 Training
To ensure the successful implementation and maintenance of the Data Protection Policy, trust staff need to be appropriately informed and trained – training is provided during Induction, prior to Clinical System Training, and by completion of Information Governance annual mandatory training.

All staff who undertake "Subject Access" processing will be required to complete the Health & Social Care Information Centre (HSCIC) e.learning module "Access To Records" on an annual basis.

6. MONITIORING COMPLIANCE

- Annual Staff survey to identify any knowledge or skills gaps with an Annual Report and action plan tabled at the Joint SIRO & Information Governance Committee.
- Annual survey undertaken with service users/carers with results included in Annual Report to Joint SIRO & Information Governance Committee.
- Development and monitoring of an “action plan” will be overseen by the Joint SIRO & Information Governance Committee
- Monitoring and review of any breaches or data loss incidents which must be reported using the Adverse Incident Reporting Policy and reporting Systems.
- Notification of any data breaches or data loss incidents via the Adverse Incident reporting systems to the Information Governance Manager.
- Review of all adverse incident reports associated with data breaches/information loss incidents at the Joint SIRO & Information Governance Committee bi-monthly meeting.
- Regular incident reports forwarded to Divisions for review/action and feedback provided to Senior Information Risk Owner and Joint SIRO & Information Governance Committee.
- Reports from Joint SIRO & Information Governance Committee and Senior Information Risk Owner submitted to the Executive Committee.
- Annual Information Governance report submitted to Trustboard.

7. DEVELOPMENT & CONSULTATION PROCESS

This policy has been developed by the Information Governance Manager. The policy has been reviewed by the Joint SIRO & Information Governance Committee which includes the Senior Information Risk Owner and Caldicott Guardian.

8. REFERENCE DOCUMENTS

Information Governance & Information Risk Trust Policy
Confidentiality & Data Sharing Trust Policy
Information Management & Technology Trust Policy.
Freedom of Information Act Trust Policy
The Data Protection Act 1998
www.hmso.gov.uk/acts/acts1998/19980029.htm
Freedom of Information Act 2000
www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1
The Caldicott Reviews of the Uses of Patient-Identifiable Information (1997) and Information Governance (2013)
Information Security Standards (BS7799)
Health and Social Care Information Centre’s Code of Practice on Confidential Information (2013)
ICO Subject Access Code of Practice (2014)

9. BIBLIOGRAPHY

No Bibliography

10. GLOSSARY

No glossary terms

11. APPENDICES

Data Protection Act Procedure – Appendix 1
Contact directory for Subject Access Requests - Appendix 2

Appendix 1

Data Protection Act – Subject Access Procedure

1. INTRODUCTION

The Data Protection Act 1998 provides individuals (Data Subjects) with the right to access their personal data, including health records. A health record is defined in the 1998 Act as being any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

The 1998 Act deals with request for access to the personal data of living individuals. The Access to Health Records Act 1990 deals with requests for access to records relating to deceased individuals.

NHS records are public records and relate to **all types of records** including:

- Patient health records (electronic or paper based concerning all specialties);
- Accident and Emergency, birth and all other registers;
- Theatre registers and minor operations (and other related) registers;
- Administrative records (including, for example, personnel, financial, estates);
- X-ray and imaging reports, output and images;
- Photographs, slides and other images;
- Microform (microfiche/microfilm);
- Audio and video tapes, cassettes, CD-ROM;
- CCTV footage
- Emails;
- Computerised records;
- Scanned records;
- Text messages (both outgoing messages from the NHS and incoming responses from the patient)

Where any of the above constitute or contain personal data under the 1998 Act they can be accessed by Data Subjects.

2. SUBJECT ACCESS REQUEST PROCEDURE

2.1 Requests should be made in writing, however a judgement to excuse this requirement may need be considered in exceptional circumstances. Applications can be from various sources including: Solicitors, Patients Medical Insurance Companies, Police requests should be accompanied by a signed written authorisation from the service user. See the Corporate Data Protection Act Policy for further information.

2.2 The Applicant (data subject) must provide enough information for the Trust to be able to process the request.

2.3 The Trust may need to confirm what information is required. This should be done using a Subject Access Application Form.

2.4 The statutory timescale for processing of each request is **40 calendar days**. However, Department of Health Policy requires that the Trust provide access to health records within 21 days.

2.5 An acknowledgement letter to the Applicant's request for access to health records is sent.

2.6 Under the DPA if a written authorisation has been signed there is no limited time period for it to be considered valid. However, the Trust would typically consider that a written authorisation signed within the preceding 12 months is valid. If in doubt, further queries should be made to ensure that the third party has lawful authority to make the request on behalf of the data subject.

2.7 All requests, including future actions taken, must be recorded via the Trusts central recording systems and retained as a Trust Corporate Record for the statutory retention period stated in the NHS Code of Practice Records Management.

2.8 All relevant information must be collated in preparation for undertaking "third party identification".

2.9 Checks must be made to ensure that all the information requested is included. For example, electronic and hardcopy records.

2.10 Consent will be obtained from treating clinicians (appropriate healthcare professional) before disclosure of the information. They may be asked to explain any unintelligible terms. Or in the case of non-clinical records these must be reviewed by a senior lead in the respective area and approved for disclosure.

2.11 The Trust may refuse to disclose all or part of the information should any of the following criteria apply:
- disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person;
- the records refer to another individual (apart from a health professional) who can be identified from that information. That is unless the other individual's consent is obtained or the records can be anonymised or it is reasonable in all the circumstances to comply with the request without that individual's consent, taking into account any relevant factors including any duty of confidentiality owed to the third party. See the Corporate Data Protection Act Policy for further information.
Confirmation of this decision is obtained from the health professional in writing and must be recorded in the step by step process in the Trust's central recording system.

2.12 If a decision is taken that the record should not be disclosed a letter must be sent by Royal Mail - Special Delivery to the patient or their representative stating the reasons for partial or non-disclosure.

2.13 The Trust recording systems must be updated at each stage of the Subject Access process.

2.14 Redaction of records must be undertaken by using a “black indelible ink marker” prior to photocopying the records. Care must be taken to ensure that any redacted information cannot be viewed on copies prepared for disclosure.

2.15 One set of copied information will be made for the applicant and a copy retained for trust information. Any redacted documentation will be retained on the trust copy. The copy prepared for disclosure must have “Subject Access Copy” either stamped or written onto the top right hand corner.

2.16 Once the appropriate documentation has been approved, the recipients address must be checked prior to a copy of the information being sent. All copy documentation must be sent in a sealed envelope by Royal Mail - Special Delivery or via secure electronic technology approved by the Trust. Original records/copies should never be sent.

2.17 Should an applicant wish to collect the copy information, a date and time for collection must be arranged and a letter of confirmation sent. The applicant will be asked to sign a collection receipt and provide proof of identity.

2.18 **Deceased Patient’s Records**: Subject to the following qualifications, the same procedure as that used for disclosing a living patient’s records should be followed when there is a request for access to a deceased patient’s records. Access can only be provided if the requestor can provide evidence that:

- They are the late persons personal representative OR Executor, OR
- Are any other person who may have a claim arising out of the individuals death

Access should not be granted if:
- the appropriate health professional is of the view that this information is likely to cause serious harm to the physical or mental health of any individual; or
- the records contain information relating to or provided by an individual (other than the patient or a health professional) who could be identified from that information (unless that individual has consented or can be anonymised); or
- the record contains a note made at the request of the patient before his/her death that he/she did not wish access to be given on application. (If while still alive, the patient asks for information about his/her right to restrict access after death, this should be provided together with an opportunity to express this wish in the notes).
- the holder is of the opinion that the deceased person gave information or underwent investigations with the expectation that the information would not be disclosed to the applicant.

2.19 **Charges –** The Trust does not levy charges for the provision of Subject Access Requests.

2.20 Any requests received under the Freedom of Information Act 2000 will be managed in accordance with the Trust’s Freedom of Information Policy and must be forwarded to the Freedom of Information Administrator or Freedom of Information mailbox.

2.21 If the Applicant is not satisfied with the information received and this cannot be resolved through the provision of further information and negotiation with the Trust Information

Governance Manager they will be advised that they have the right to contact the Information Commissioner for a case review.

Appendix 2

Subject Access Request – Division Contacts

SECURE DIVISION

(Ashworth Hospital & Scott Clinic)

Health Records Manager,
Ashworth Hospital,
Parkbourn,
Maghull.
Liverpool
L31 1HW

(Low Secure Unit)

Ward Clerk
Low Secure Unit,
Rathbone Hospital,
Mill Lane,
Liverpool
L13 4AW

LOCAL DIVISION

Patient Appointments Centre
Norris Green Community Hub,
Falklands Approach,
Liverpool,
L11 5BS

General Office Supervisor,
Mossley Hill Hospital,
Park Avenue,
Liverpool,
L18 8BU.

Access to Records Clerk (Learning Disabilities or Adult Mental Health)
Hesketh Centre,
Albert Road,
Southport.
PR9 OLT

Addictions

Secretary to Consultant Psychiatrist/Clinical Director
Windsor House,
Upper Parliament Street, Liverpool.

CORPORATE DIVISION

Human Resources Department,

Head of Workforce Development,
Mersey Care NHS Trust,
V7 Building,

Kings Business Park,
Prescott,
Liverpool
L34 1PJ.

Occupational Health Department/Staff Support
Occupational Health Department/Staff Support
Mersey Care NHS Trust,
Switch House,
Northern Perimeter Road,
Bootle,
Liverpool
L30 7PT

CALDERSTONES – Specialist LD Division
Health Records Department
Mitton Rd,
Whalley,
Lancs,
BB7 9PE

Human Resources
Mitton Rd,
Whalley,
Lancs,
BB7 9PE

Implemented: October 2012
Review: December 2016

APPENDIX 3

REQUEST FOR DISCLOSURE OF SERVICE USER RECORDS IN CONNECTION WITH DISCIPLINARY PROCEEDINGS

This form must be completed by managers and/or staff side representatives **BEFORE** accessing service user records for the purposes of disciplinary hearings. Please be as specific as possible and provide all necessary information in order to facilitate timely decision making and avoid unnecessary delays. The person requesting access should complete section A and then submit their request via email to a senior HR advisor. A separate table should be completed for each document/record requested. Additional tables should be added accordingly.

SECTION A: RECORDS REQUESTED

Health Record / Document Requested:	
Date(s):	
Rationale for disclosure:	

Health Record / Document Requested:	
Date(s):	
Rationale for disclosure:	

Health Record / Document Requested:	
Date(s):	
Rationale for disclosure:	

SECTION B: HUMAN RESOURCES

Date Received in HR:	
Received by:	

Equality and Human Rights Analysis

Title: Corporate Data Protection Act Policy
Area covered: Trust wide

What are the intended outcomes of this work? *Include outline of objectives and function aims* To issue guidance to everyone working with Personal Identifiable information, regardless of what media it is retained in; outline current legislation details in the DPA; responsibilities of the Trust and it's employees.
Who will be affected? *e.g. staff, patients, service users etc* Patients / service users, staff

Evidence
What evidence have you considered? The protection of Personal Identifiable information and the framework for application of DPA.
Disability inc.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.*

Human Rights	**Is there an impact?** **How this right could be protected?**

Right to life (Article 2)	
Right of freedom from inhuman and degrading treatment (Article 3)	
Right to liberty (Article 5)	
Right to a fair trial (Article 6)	
Right to private and family life (Article 8)	
Right of freedom of religion or belief (Article 9)	
Right to freedom of expression Note: this does not include insulting language such as racism (Article 10)	
Right freedom from discrimination (Article 14)	

Engagement and involvement

Summary of Analysis The policy is robust and evidence shows no potential for discrimination.
Eliminate discrimination, harassment and victimisation
Advance equality of opportunity
Promote good relations between groups
Addressing the impact on equalities

Action planning for improvement

None required

Please give an outline of your next steps based on 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:

Gina Kelly, Lee Ellison, Kate Greenwood

Date assessment completed:

7th August 2012

Name of responsible Director/Director General:

Medical Director

Date assessment was signed:
7th August 2012

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 Directorate
Involvement and consultation			
Data collection and evidencing			
Analysis of evidence and assessment			
Monitoring, evaluating and reviewing			
Transparency (including publication)			

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Co-ordination of implementation • How will the implementation plan be co-ordinated and by whom? *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 Information 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.	Nov 2015
Engaging staff • Who is affected directly or indirectly by the policy? • Are the most influential staff involved in the implementation? *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 • Is there a need to provide information to service users and carers regarding this policy? • Are there service users, carers, representatives or local organisations who could contribute to the implementation? *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. • Service Users and Carers will not be involved in implementing the procedure.	

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Communicating • What are the key messages to communicate to the different stakeholders? • How will these messages be communicated? *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: - That all staff must comply with current legislation outlined within the Data Protection Act 1998 and the NHS Code of Confidentiality. • All staff will be able to access the policy via their manager or the Trust website.	
Training • What are the training needs related to this policy? • Are people available with the skills to deliver the training? *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 Trust Induction and Corporate Essential Training • Staff will receive information regarding DPA Act & their responsibilities prior to being provided with "live" access to the Clinical Information Systems. Staff must complete the Information Governance training mandatory modules upon commencement with the Trust & then annually. Training will be on-line via the Connecting for Health IG training tool/ESR. Training completion will be overseen by the Information Governance Manager and monitored via IGC.	Annually

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Resources • Have the financial impacts of any changes been established? • Is it possible to set up processes to re-invest any savings? • Are other resources required to enable the implementation of the policy eg. increased staffing, new documentation? *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.	
Securing and sustaining change • Have the likely barriers to change and realistic ways to overcome them been identified? • Who needs to change and how do you plan to approach them? • Have arrangements been made with service managers to enable staff to attend briefing and training sessions? • Are arrangements in place to ensure the induction of new staff reflects the policy? *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.	

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Evaluating • What are the main changes in practice that should be seen from the policy? • How might these changes be evaluated? • How will lessons learnt from the implementation of this policy be fed back into the organisation? *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 Data Protection Act and staff's responsibilities to comply with this and the NHS Code of Confidentiality. • Annual completion of Information Governance training – audited as part of the Information Governance Toolkit compliance • Surveys will also be conducted with Service Users & staff to ensure they are aware of their rights & understand the legislation. The results of the surveys will be monitored and reviewed by the Information Governance Committee on an annual basis.	March annually
Other considerations		