Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL POLICY

CORPORATE DATA PROTECTION ACT 2018 GENERAL DATA PROTECTION REGULATION POLICY

Policy Number:	**IT14**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO and Information Governance Group**
Approved by:	**Executive Director of Finance**
Date Ratified:	**June 2020**
Next Review Date (by):	**May 2021**
Version Number:	**2020-Version 8**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Information Governance Officer**

TRUST-WIDE NON-CLINICAL POLICY

May 2020 –Version 8

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL POLICY

CORPORATE
GENERAL DATA PROTECTION REGULATION 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 General Data Protection Regulation, Data Protection Act 2018 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	Geoff Springer Information Governance Officer Geoff.Springer@merseycare.nhs.uk 0151 478 6899
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **V7 Building,** **Kings Business Park,** **Prescot,** **Liverpool.** **L34 1PJ** **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 4		May 2016
Version 5		January 2018
Version 6	Policy Group	December 2018
Version 7		December 2019
Version 8	Executive Director of Finance Approval	June 2020

NHS
Mersey Care
NHS Foundation Trust
Community and Mental Health Services

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 adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / 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 / 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 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, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not 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

1. Purpose and Rationale

1.1 **Rationale**
Mersey Care NHS Foundation Trust acknowledges the importance of good practice regarding management of personal data and endorses the principles of data protection. In addition, this policy outlines the general managerial policy and approach to embedding good data protection practice within the Trust.

1.1.2 The Data Protection Act 2018 and the General Data Protection Regulation came into force in May 2018. Together, they entitle a living individual, with certain exceptions, to view or be provided with copies of their personal data. The legislation covers both manually or electronically recorded data and includes, amongst other matters, the right for an individual to know the purposes for which their data is being processed, and with whom personal data is shared and the lawful basis for sharing. A personal request for personal data under the Act is commonly known as a Subject Access Request.

1.1.3 The Data Protection Act 2018 and the General Data Protection Regulation only apply to information held about living individuals.

1.1.4 There is provision for requests relating to the deceased under the Access to Health Records Act 1990.

2. Scope

2.1 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.

2.2 This policy endorses and complies with NHS Digital Code of Practice on Confidential Information, the Caldicott Review regarding the uses of patient-identifiable information (1997), Information Governance Review (2013), National Data Guardian review and guidance issued by the Information Commissioner's Office which concerning the processing, use and disclosure of personal data.

- It will provide a framework within which the Trust will ensure compliance with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation.
- It will underpin any operational procedures and activities connected with the implementation of the Regulation.

3.0 Outcome Aims and Objectives

3.1 The Trust needs to collect and use certain types of information about people with whom it deals in order to operate. In addition, it may occasionally be required by law to collect and use certain types of information to comply with legal requirements. This includes 'personal data' as defined by the Data Protection Act 2018 and the General Data

Protection Regulation.

3.1.2 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 and Regulation. This includes information about current, past and prospective employees, suppliers, patients, and others with whom it communicates.

3.1.3 This personal data 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 and the General Data Protection Regulation. The Trust must comply with both the Act and Regulation. The Trust regards the lawful and correct treatment of personal data as very important to providing services and to maintaining confidence between partnership organisations and its service users. The Trust ensures that personal data fully endorses and adheres to the principles of data protection, as defined in the Data Protection Act 2018 and the General Data Protection Regulation.

3.1.4 Specifically, the principles set out in the Regulation require that personal data:

- shall be processed lawfully, fairly in a transparent manner in relation to the data subject;
- shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes;
- shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- shall kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

and that:

- personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- the controller shall be responsible for, and be able to demonstrate compliance with, all of the Data Protection principles.

3.1.5 The Data Protection Act and the General Data Protection Regulation put strict controls on the use of personal data. In order to enforce this, the Chief Executive has overall responsibility for compliance where the Trust is the data controller. The implementation of compliance is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer and other designated staff.

4.0 Definitions

The provisions of the Data Protection Act 2018 and the General Data Protection Regulation apply only to personal data. The term **'personal data'** is defined as data which relate to a living individual who is identified or who can be identified, directly or indirectly. Such identification might be by an identifier such as a name, an identification number, location data or online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

4.1 **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 and Regulation. The Trust is expected to be the data controller in respect of the vast majority of personal data that it holds (e.g. personal data about service users and employees).

4.2 **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 clinical record, the service user to whom it relates will be the data subject.

4.3 **Filing System**
A 'filing system' is defined in section 3(1) of the Act as: any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis. 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 it is subject to the requirements of the Act and Regulation.

4.4 **Health Record** – A 'health record' is defined in section 205(1) of the Act as being any record which consists of data concerning health and has been made by or on behalf of a healthcare professional in connection with the diagnosis, care or treatment of the individual to whom the data relates. 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.

4.5 **Health Professional** – A health professional is defined in section 204 of the Act as:

- A registered medical practitioner;
- A registered nurse or midwife;
- A registered dentist as defined by section 53 of Dentists Act 1984;

- A registered dispensing optician or registered optometrist as defined by section 36 of the Opticians Act 1989;
- A person registered as a member of a profession to which the Health and Social Work Professions Order 2001 for the time being extends, other than the social work profession in England;
- A registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010;
- A registered person as defined by Article 2 of the Pharmacy (Northern Ireland) Order 1976;
- 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;
- A child psychotherapist;
- A scientist employed by a health service body as a head of department.

5. Process

5.1 Access to Personal Data

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

5.1.1 **The data subject** is entitled to make a request for any personal data held about them under the Act and Regulation. 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 or Regulation 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 by a data subject for their personal data, whether verbally or in writing (e.g. letter, email, fax, social media post) to any Trust employee will be classed as valid.

5.1.2 If an applicant makes their request verbally to a Trust representative, the Trust representative will note the required information to deal with the request on a Trust approved form for processing.

5.1.3 In all cases the Trust **must** ensure that the identity of the applicant is determined before disclosure is made.

5.2 A person with written authorisation to act on behalf of the data subject (including solicitors instructed on behalf of the data subject, etc.)

5.2.1 Anyone making a Subject Access Request on behalf of someone else must ensure that they have valid, applicable, written authorisation (such as a consent form from the data subject in their favour, which must be signed by the data subject) which is provided to the Trust.

5.2.2 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 document must be provided in such cases.

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

5.3.1 Where a service user lacks capacity to make a Subject Access Request themselves, someone appointed to act on their behalf under a valid and applicable Power of Attorney for Health & Wellbeing (an Attorney) or by the courts (a Deputy) may submit a subject access request on behalf of the data subject.

5.3.2 An attorney must provide proof of the Power of Attorney for Health & Wellbeing which is a standard document that must have been registered with the Office of the Public Guardian before it can be used.

5.3.3 A Deputy must provide a sealed copy of the court order appointing them as a deputy.

5.3.4 Where in any doubt as to the validity of such documents or the limitations that might apply to the attorney or deputy's appointment, further legal advice should be sought.

5.4 A person acting on behalf of a child

5.4.1 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.

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

5.4.3 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 and Regulation. If you are confident that the child can understand their rights, then you should respond to the child directly. The Trust may however allow a parent to exercise a child's right if the child has authorised that parent to do so. If the child is unable to understand their rights under the Act, then someone with parental responsibility can make the request on their behalf in their best interests.

5.4.4 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.

5.5 The Police

5.5.1 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).

5.5.2 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 data protection legislation 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.

5.5.3 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. In accordance with the Data Protection Act 2018, schedule 2, Part 1 paragraph 2 and that processing is on the grounds of the General Data Protection Regulation Article 6(1)(d) or (e) and Article 9(2)(g). The Trust has to be satisfied that these grounds are met and only relevant and proportionate information should be disclosed.

5.5.4 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 template request forms are held and should be completed by police forces and provided to the Trust before the disclosure. If the form has not been properly completed or provides insufficient information, the Trust will seek clarification from the police as required.
- Consider whether it is appropriate to get the individual's agreement 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 agreement may "tip them off"). In such cases the police must explain in writing why seeking agreement would in fact prejudice their investigation or otherwise be inappropriate, which should be documented by way of an audit trail.
- Subject to the above, in any case involving a patient, it is good practice to consult with the patient to obtain their agreement, where possible, particularly where there may be an ongoing therapeutic relationship. The potential impact on the patient of seeking agreement or making a disclosure without such agreement 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 agreement to disclosure then, in the absence of this, the Trust must be satisfied that it is justified and lawful 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. A 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 and reasons for disclosure 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.

5.6 Court Order or Coroners Request

5.6.1 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.

5.6.2 Court Orders directing disclosure do not require prior consent from the data subject and **must be** actioned immediately. However, the Trust should ensure that the Court Order is sealed and dated and that the requirement on the Trust to disclose specific personal data and to whom is clear. The Trust will contact the Court should it have any doubts as to its validity or what is required.

5.6.3 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.

5.6.4 If the Trust receives a request from the Coroner then these requests must be actioned immediately and do not constitute a Subject Access Request. Note that the General Data Protection Regulation does not apply to deceased individuals – discussed further below.

5.7 Appointed Representative of the Deceased

5.7.1 The Data Protection Act 2018 and the General Data Protection Regulation do 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.

5.7.2 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 executor of the will, personal representative with letters of administration or any person who may have claim on the estate arising out of the service user's death.

5.7.3 The personal representative (executor or administrator – 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 and relies upon their potential claim, they should detail why they need access to the records in pursuing that claim. Where they are the executor or administrator they must provide proof of appointment under the Will/Grant of probate.

5.8 Timetable for Access

5.8.1 For living individuals, the Data Protection Act 2018 and the General Data Protection Regulation require Subject Access requests to be complied with within 1 calendar month. However, under Department of Health policy, whenever possible the requests for medical records should be dealt with within 21 days.

5.9 Providing Information

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

- Check for any third party information and consider whether it should be removed before disclosure or whether the necessary consent has been obtained from the third party to disclose or it is otherwise lawful to disclose that third party data (see further below);
- 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 4.16 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 Royal Mail - Special Delivery or collected in person by the applicant or sent out electronically via the Trust secure protocol.

5.9.2 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).

5.9.3 In such circumstances the consent of the third party to disclose 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:

- the type of information that would be disclosed;
- 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 express refusal of consent by the third party individual.

5.10 Explanation of the Data

5.10.1 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 support.

5.10.2 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 or received an individual's electronic personal confidential data, should be made available in a suitable form to patients.

5.11 The Right to Rectification (Inaccuracies in Health Records)

5.11.1 Any requests for alleged inaccuracies within the record to be corrected will only be made in conjunction 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.

5.11.2 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.

5.11.3 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.

5.12 The Right to Erasure

5.12.1 Under Article 17 of the General Data Protection Regulation individuals have the right to have personal data erased in certain circumstances. This is also known as the "right to be forgotten". This right is not absolute.

5.12.2 Individuals have the right to have their personal data erased if:-

- the personal data is no longer necessary for the purpose which it was originally collected or processed;
- consent was being relied upon as the lawful basis for processing the data, and the individual withdraws their consent;
- the individual objects to the processing of their data under Article 21(1) of the General Data Protection Regulation, and there is no overriding legitimate interest to continue this processing;
- the personal data was being processed for direct marketing purposes and the individual objects to that processing;
- the personal data has been processed
- personal data must be erased to comply with a legal obligation; or
- the personal data was processed to offer information society services to a child

5.12.3 However, there are limits to the right set out in Article 17(3), such as where processing is necessary to comply with a legal obligation of the Trust or for the performance of a task carried out in the public interest or in the exercise of official authority or necessary for the establishment, exercise or defence of legal claims.

5.13 The Right to Restrict Processing

5.13.1 Article 18 of the the General Data Protection Regulation gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This right could be used by data subjects as an alternative to, or prior to, requesting the erasure of their data.

5.13.2 Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction set out in Article 18(1), such as whilst they contest the accuracy of the data and whilst the Trust verifies if the data is accurate. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

5.14 The Right to Data Portability

5.14.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services in certain situations.

5.14.2 It assists them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

5.14.3 The right allows a data subject to receive his or her personal data, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and to transmit that data to another controller without hindrance from the controller to whom the data had been provided.

5.14.4 The right only applies where processing of the personal data was on the grounds of consent or on a contract with the data subject and where processing is carried out by automated means.

5.15 The Right to Object

5.15.1 Article 21 of the the General Data Protection Regulation gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.

5.15.2 The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

5.15.3 Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

5.15.4 Individuals can also object if the processing is for:

- a task carried out in the public interest or;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

5.15.5 In these circumstances the right to object is not absolute and does not apply if the Trust demonstrates overriding, compelling legitimate grounds for the processing or for the establishment, exercise or defence of legal claims.

5.15.6 If processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

5.16 Exemptions

5.16.1 There are a number of exemptions to rights under the the General Data Protection Regulation, including the right of access. Where access is to be denied in accordance with an exemption the applicant will be informed of this.

5.16.2 One such exemption of particular relevance to the Trust is the exemption under the Data Protection Act 2018 Schedule 3 paragraph 5. This exemption applies where disclosure is likely to cause serious harm to the physical or mental health of the data subject, or someone else. This decision would be made by the appropriate healthcare professional as defined in that Schedule.

5.17 Management and Completion of Subject Access Requests

5.17.1 Administrative staff processing Subject Access Requests **must** ensure that all Subject Access Requests are lodged onto the Trust central recording database. 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 Joint SIRO & Information Governance Group 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, legal challenge or as evidence for the Information Commissioner's Office.

5.18 Fees

No fees are levied for Subject Access Requests as per the Data Protection Act 2018 and the General Data Protection Regulation.

5.19 National Data Opt-out Policy

A secure and accessible tool for people to opt-out of their confidential patient information being used for reasons other than their individual care and treatment is available. This means patients have more control over how their information is used and gives them the opportunity to make informed choices about whether they wish their confidential patient information to be used just for their individual care and treatment or also used for research and planning purposes. Further information is available at https://www.nhs.uk/your-nhs-data-matters/. When necessary, the Trust applies the Policy to its data.

You can also opt-out of the national screening programmes. For further information, please go to https://www.gov.uk/government/publications/opting-out-of-the-nhs-population-screening-programmes.

6 Duties and Responsibilities

6.1 Trust Responsibilities

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

- observe fully conditions regarding the lawful and fair collection and processing of information;
- meet its legal obligations to specify the purposes for which information is used;
- ensure that the Trust has Privacy Notices available for service users, employees and others (including in Easy Read format) to inform individuals about the processing of their personal data.
- collect and process appropriate information, only to the extent that it is needed to fulfill 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 Information Governance Alliance Records Management Code of Practice for Health & Social Care;
- ensure that the rights of people about whom information is held can be fully exercised in accordance with the Regulation (These include: the right to be informed where processing is being undertaken: the right of access to one's personal data; the right to object to processing in certain circumstances; the right to rectify, restrict or erase certain personal data and the right to data portability);
- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred outside of the The Union without suitable safeguards.

In addition, the Trust will take steps to ensure that:

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

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

6.1.3 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.

6.1.4 All data loss or data breach incidents will be reviewed and monitored by the Joint SIRO and Information Governance Group. Individual incidents will be managed in relation to assessment against the relevant legislation and Information Commissioner's reporting criteria and reported as required. Individuals involved in data loss/breach incidents will be formally written to and advised of the incident by the Trust which may involve discussion with clinical teams.

6.1.5 Please refer to the Trust policies and procedures for disclosure of information in response to Freedom of Information requests which relate directly to the Trust organisational business.

6.2 Roles

6.2.1 Senior Information Risk Owner

The Senior Information Risk Owner (Executive Director of Finance) is responsible for ensuring that the Trust manages its information assets securely and has taken appropriate action to mitigate against any data loss/data breach incidents and that all data loss/data breach incidents are monitored and reviewed.

6.2.2 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility in ensuring that a robust framework to comply with all legislation is in place across the Trust. It is the responsibility of the Caldicott Guardian to ensure that every member of staff within the Trust complies with all requirements of Information Governance, which is driven by various legislation and guidelines issued by the Department of Health and other sources.

6.2.3 Data Protection Officer

The Data Protection officer is responsible for:-

- Overseeing the overall management of the Subject Access Requests process.
- Promoting data protection advice and awareness for service users and employees
- Investigating breaches of data protection and confidentiality audits
- Liaising with the Information Commissioner's Office on behalf of the Trust including ensuring arrangements are in place for the payment of any fees; and
- Providing regular monitoring compliance against legislation reports to the Executive Committee.

6.2.4 Senior Managers

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

6.2.5 All Staff

- Must understand their legal obligation to keep personal data 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, Senior Information Risk Owner Lead and Data Protection Officer and be aware of the "lead" within their Division whom they should liaise with regarding confidentiality issues;
- 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 legislation 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; and
- To ensure data is recorded accurately and in a legible manner.

7. Training and Support

To ensure the successful implementation and maintenance of the General Data Protection Regulation Policy, Trust staff need to be appropriately informed and trained – training is provided during induction, prior to clinical system training, and by completion of the Data Security Awareness Training module endorsed by NHS Digital.

8. Monitoring

- Annual Staff survey to identify any knowledge or skills gaps with an Annual Report and action plan tabled at the Joint SIRO & Information Governance Group.
- Annual survey undertaken with service users/carers with results included in Annual Report to Joint SIRO & Information Governance Group.
- Development and monitoring of an "action plan" will be overseen by the Joint SIRO & Information Governance Group.
- 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 Data Protection Officer.
- Review of all adverse incident reports associated with data breaches/information loss incidents at the Joint SIRO & Information Governance Group 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 Group.
- Reports from Joint Siro & Information Governance Group and Senior Information Risk Owner submitted to the Executive Committee.
- Annual Information Governance report submitted to Trust Board.

9. Consultation Process

This policy has been developed by the Information Governance Officer/Data Protection Officer. The policy has been reviewed by the Joint SIRO & Information Governance Group which includes the Senior Information Risk Owner and Caldicott Guardian.

10. Appendices:

Reference Documents – Appendix 1
Data Protection Act Procedure – Appendix 2
Contact directory for Subject Access Requests - Appendix 3

Appendix 1

Reference Documents

Information Governance & Information Risk Trust Policy
Confidentiality & Data Sharing Trust Policy
Information Management & Technology Trust Policy.
Freedom of Information Act Trust Policy
Data Protection Act 2018
Freedom of Information Act 2000
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)
CO Subject Access Code of Practice (2014)
General Data Protection Regulation (2018)

Appendix 2

Data Protection Act – Subject Access Procedure

1. INTRODUCTION

1.1 The Data Protection Act 2018 and the General Data Protection Regulation provide living individuals (Data Subjects) with the right to access their personal data, including health records. (The Access to Health Records Act 1990 deals with requests for access to records relating to deceased individuals.) A health record is defined in the Data Protection Act as any record which consists of data concerning health and has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

NHS records can comprise **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 General Data Protection Regulation and Data Protection Act they can be accessed by Data Subjects (service users, employees or their authorised representatives).

2. SUBJECT ACCESS REQUEST PROCEDURE

2.1 Requests do not need to be made in writing; however verbal requests will be recorded by the Trust by way of an audit trail. Requests can be made from various sources on behalf of a data subject including: solicitors, patients medical insurance companies, police. Requests made on behalf of a data subject should be accompanied by a signed written authorisation from the service user before being processed. 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 ask the data subject to confirm what information is required. This should be recorded using a Subject Access Application Form.

2.4 The statutory timescale for processing of each request is without undue delay and in any event within **one calendar month**. 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 upon receipt.

2.6 If a written authorisation from the data subject has been signed there is no pre-determined time period after which it will no longer be considered valid and authorisations will be considered on a case by case basis. However, as a general rule, 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 Information Governance Alliance Records Management Code of Practice for Health & Social Care.

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. Confirmation of this decision is obtained from the health professional in writing and must be recorded in the step by step process in Datix.

- 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.

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 records. 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. 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 Royal Mail - Special Delivery or collected in person by the applicant or sent out electronically via the Trust secure protocol. 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
- They 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, local discussion and negotiation with the Trust's Data Protection Officer, they have the right to contact the Information Commissioner for a case review.

Appendix 3

Subject Access Request – Division Contacts

SECURE DIVISION

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

LOCAL DIVISION

Access to Records Team
Patient Appointments Centre
Norris Green Community Hub,
Falklands Approach,
Liverpool,
L11 5BS

Talk Liverpool
Admin - Access Team
Talk Liverpool
7 New Hall
Fazakerley
Liverpool
L10 1LD

WHALLEY SITE – Specialist LD Forensic Division

Health Records Department
Mitton Rd,
Whalley,
Lancs,
BB7 9PE

LIVERPOOL & SEFTON COMMUNITY DIVISION

Information Governance Department
Liverpool Innovation Park,
2ND Floor Digital Way,
Liverpool,
L7 9NJ.

CORPORATE DIVISION

Human Resources Department.

Head of Workforce Development,
Mersey Care NHS Foundation Trust,
V7 Building,
Kings Business Park,
Prescot,
Liverpool
L34 1PJ.

Occupational Health Department/Staff Support

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

I

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. 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.	
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 Foundation 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 services users or carers with a copy of this policy However it will be available on via the Trust's website or copies will be provided upon request in different formats. Also how we use service user's information is detailed in the Trust's Privacy Notice, which is also available on the Trust's website. Service Users and Carer 's 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 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 Data Protection Officer and monitored via Joint Siro & Information Governance Group.	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 Joint SIRO & Information Governance Group on an annual basis.	March annually
Other considerations