Trust-wide Document

Great Western Hospitals NHS Foundation Trust

Data Protection Policy

Document No	IG - 00011	**Version No**	1.0
Approved by	Policy Governance Group	**Date Approved**	07/07/2021
Ratified by	Information Governance Steering Group	**Date Ratified**	02/07/2021
Date implemented (made live for use)	19/07/2021	**Next Review Date**	02/07/2024
Status	LIVE		
Target Audience- who does the document apply to and who should be using it. - The target audience has the responsibility to ensure their compliance with this document by: • Ensuring any training required is attended and kept up to date. • Ensuring any competencies required are maintained. • Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.	All employees directly employed by the Trust whether permanent, part-time or temporary (including fixed-term contract). It applies equally to all others working for the Trust, including private-sector, voluntary-sector, bank, agency, locum, and secondees. For simplicity, they are referred to as 'employees' throughout this policy		
Special Cases	None		
Accountable Director	Medical Director / Caldicott Guardian		
Author/originator – Any Comments on this document should be addressed to the author	Information Governance Manager / Data Protection Officer		
Division and Department	Finance / Corporate		
Implementation Lead	Information Governance Manager / Data Protection Officer		
If developed in partnership with another agency ratification details of the relevant agency	n/a		
Regulatory Position	General Data Protection Regulation (UK and EU) (Ref 2) Data Protection Act 2018 (Ref 3) Health and Social Care (Safety and Quality) Act 2015 (Ref 7)		
Review period. This document will be fully reviewed every three years in accordance with the Trust's agreed process for reviewing Trust -wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.			

Contents

1 Introduction & Purpose 3
1.1 Introduction & Purpose 3
1.2 Glossary/Definitions 3
2 Main Document Requirements 4
2.1 Data Protection Act 2018 Principles 4
2.2 Lawful Basis for Processing Data 5
2.3 Data Protection Impact Assessments (DPIA) 6
2.4 Rights of Data Subjects 6
2.5 Disclosure 7
2.6 Exemptions Allowing Disclosure 7
2.7 Subject Access Requests 7
2.7.1 Health Records 8
2.7.2 Non-Health Records 8
2.7.3 Access to Email 8
2.7.4 Third Party Information 8
2.7.5 Closed-Circuit Television (CCTV) Images 9
2.7.6 Charges for Subject Access Requests 9
2.8 Data Controller Register 9
3 Monitoring Compliance and Effectiveness of Implementation 11
4 Duties and Responsibilities of Individuals and Groups 12
4.1 Chief Executive 12
4.2 Ward Managers, Matrons and Managers for Non Clinical Services 12
4.3 Document Author and Document Implementation Lead 12
4.4 Caldicott Guardian 12
4.5 Senior Information Risk Owner (SIRO) 12
4.6 Data Protection Officer 12
4.7 The Information Governance Steering Group (IGSG) 12
4.8 Information Asset Owners (IAOs) / Information Asset Administrators (IAAs) 13
4.9 All Employees 13
5 Further Reading, Consultation and Glossary 13
5.1 References, Further Reading and Links to Other Policies 13
5.2 Consultation Process 13
6 Equality Impact Assessment 14
Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment 15
Appendix B – Lawful Basis for Processing Information Flowchart 17

Instant Information 1 – Trust Privacy Notices

In accordance with data protection laws, Great Western Hospitals NHS Foundation Trust (the Trust) has to be open and transparent with its employees, patients and the public about the use of personal information that it holds. This includes providing clear communications about how this information is collected, used, stored and shared. The Trust has available on its external website three privacy notices – one for patients, one for children and one for staff (Ref 1).

If an employee receives an enquiry from a patient or member of the public, or would like to know more about how their own personal information is used, they should refer to the privacy notices in the first instance.

Under the UK General Data Protection Regulation (GDPR) [Ref 2] and the Data Protection Act 2018 (DPA 2018), a data controller (that is to say an organisation that determines the purposes for which and the means by which personal data is processed) must appoint a Data Protection Officer (DPO). This person's role is to be involved properly and in a timely manner with all issues which relate to the protection of personal data. In this Trust, the person appointed to this role is the Head of Information Governance who may be contacted on: 01793 605675 or email: gwh.info.gov@nhs.net.

1 Introduction & Purpose

1.1 Introduction & Purpose

This document provides clear guidance concerning data protection within the Trust, and describes the legal obligations and responsibilities for the Trust as a whole, and for individual employees. It also describes the process necessary to renew the Trust's Data Protection registration, identifies responsible persons, and describes the Trust's purposes for processing personal information.

Both the DPA 2018 (Ref 3) and the UK GDPR give individuals (data subjects) a right of access to their personal information, including the right to request a copy of the information held, and provide a framework to ensure that personal information is handled properly. Data protection laws relate to personal information concerning living individuals.

All employees of the Trust have responsibilities regarding data protection as most process, or will process, personal and/or confidential information during the course of their work.

The DPA 2018, Human Rights Act 1998 (Ref 4) and the Freedom of Information Act 2000 (Ref. 5) are interlinked. They are intended to help maintain a fair balance between the rights and interests of individuals, in particular between the freedom to process information on the one hand and rights of privacy on the other.

The Information Commissioner's Office (ICO), an independent public body that reports directly to Parliament, sponsored by the Department for Media, Culture and Sport, is responsible for upholding information rights and enforcing data protection laws. Under UK data protection laws, the ICO is the supervisory authority for the UK.

1.2 Glossary/Definitions

The following terms and acronyms are used within the document:

ANPR	Automatic Number Plate Recognition
ARAC	Audit, Risk and Assurance Committee
CCTV	Closed Circuit Television
CQC	Care Quality Commission
CSV file	Comma Separated Values file (Microsoft Excel)
Data Controller	Organisation that is the owner of the data and makes decisions of its use
Data Processor	Organisation that complies with instructions of data controller and is liable for their actions
Data Subject	Person to whom information relates
Data/Information	Personal data is information that relates to an identified or identifiable individual
DOB	Date of Birth
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection toolkit
EIA	Equality Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
GMC	General Medical Council
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ID	Identification

IG	Information Governance
IGSG	Information Governance Steering Group
IT	Information Technology
NHS	National Health Service
NMC	Nursing Midwifery Council
Processed/Processing	Processing means any operation or set of operations which is performed on personal data; such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
RFI	Request for Information
SARs	Subject Access Request
SIRO	Senior Information Risk Owner
Special Category of Data (formerly personal sensitive data)	Special category data is more sensitive, and so needs more protection. This includes personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
UK	United Kingdom

2 Main Document Requirements

The UK GDPR was brought into force upon the UK leaving the European Union. This means organisations have to comply with this regulation and organisations have to look to the GDPR for most legal obligations. It is important that the UK GDPR and the DPA 2018 are read side by side because:

The DPA 2018 covers:

- Processing that does not fall within EU law;
- Transposing the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK Law. It sets out the requirements for the processing of personal data for criminal law enforcement purposes;
- Provisions for national security;
- The function performed by the ICO and its duties and powers to enforce data protection laws.

2.1 Data Protection Act 2018 Principles

The DPA 2018 sets out six principles that must be followed when processing data. Everyone that processes information is responsible for ensuring that they adhere to these principles:

Data must be:

- Processed in a lawful, fair and transparent manner;
- Collected for a specific, explicit and legitimate purpose and not processed in a manner that is incompatible with this purpose;
- Adequate, relevant and not excessive in relation to the purpose for which it is collected;
- Accurate and kept up to date, where necessary;
- Kept for no longer than necessary for the purpose for which it is processed;
- Processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

The DPA 2018 Act also states that the Trust "shall be responsible for, and be able to demonstrate compliance with the principles of accountability". This includes ensuring that there is a named Data Protection Officer (DPO), there is an integrated process of assessing privacy impact, known as Data

Protection by Design, and that the Trust reports and acts upon incidents. See sections below for further detail on these.

2.2 Lawful Basis for Processing Data

Under the UK GDPR, as enacted by the DPA 2018 and the European Union (Withdrawal) Act 2018 (Ref 13), in order to process personal data there must be a valid lawful basis. There are six available lawful bases for processing. No single basis is 'better' or more important, and the application will depend on the purpose trying to be achieved. The GDPR has not replaced the common law duty of confidentiality or the Caldicott Principles (Ref 8), which require the processing of personal data to be necessary. If there is an alternative, where personal data is not needed, this should be the preferred option.

If a new process is being implemented then a Data Protection Impact Assessment (DPIA) must be completed, see Section 3.3 below, and the result documented. Existing processes should be reviewed routinely as the lawful basis should not change over time. A new assessment should be completed if it has changed.

Article 9(2) of the UK GDPR recognises that special category data, which includes healthcare data, can be used in certain circumstances. However, the law explicitly states that Article 9(2) cannot be used without applying one of the lawful bases for processing, which are set out in Article 6. Before processing personal data, one of these must apply:

(a) **Consent:** the individual has given clear consent for their personal data to be processed for a specific purpose.

To be valid, the consent must be informed, give the individual a choice, provide an active opt in process, not force someone to consent, provides the individual a chance to opt out or withdraw consent, and informs them of who the data controller is.

The age of consent is 18 years old. If a child is competent then it is appropriate to let the child act for themselves. However, if a child is not competent, an individual with parental responsibility should act on their behalf.

(b) **Contract:** the processing is necessary for a contract that is in place with the individual, or because they have asked the data controller to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for to comply with the law (not including contractual obligations). An example of this could be to comply with a Court Order, provide information to the Ombudsmen during an investigation, or to assist a regulator, such as the General Medical Council (GMC), in a professional hearing.

(d) **Vital interests:** the processing is necessary to protect someone's life. This must only be used when it is not possible to ask for consent.

(e) **Public task:** the processing is necessary to perform a task in the public interest or for the Trust's official functions. As a public authority, direct healthcare services that the Trust provides will fall under this lawful basis.

(f) **Legitimate interests:** the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data. This cannot apply to healthcare services or activities of the Trust.

A Lawful Basis Flowchart is attached at Appendix B to assist in determining which lawful basis may apply. The basis must be confirmed before processing the data and should be documented where necessary; for example, on consent forms, as part of a signed contract, in the medical record.

2.3 Data Protection Impact Assessments (DPIA)

A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies. The UK GDPR legislates that privacy assessments are mandatory, whereas prior to May 2018 they were recommended.

The Data Protection Impact Assessment is split into two sections; the initial screening tool and the full DPIA assessment.. A template for the DPIA and guidance on completion of the assessment may be requested from the Information Governance Team.

The screening tool must be completed for all new data processes. If the screening tool identifies that there is a need for a full assessment, this must be completed before the new process/project is implemented. Any risks identified by the DPIA must be listed at the end of the form, with agreed actions to mitigate this risk.

The Data Protection Officer or a member of the Information Governance (IG) team must be consulted at the earliest opportunity to ensure that privacy and the lawful basis for processing data have been correctly established into the project design. If the processing of information involves a third party or a new electronic system, a further information sharing agreement or information asset security assessment may need to be completed in addition to the DPIA.

The DPIA must be approved at the appropriate level to the project and the report and/or summary must be made available to the appropriate stakeholders, such as through a directory on the Trust's website. The DPIA register is a standing item at the Information Governance Steering Group, which has delegated responsibility to manage this process.

2.4 Rights of Data Subjects

Under data protection law there are several rights for the data subject:

- The right to be informed about whether an organisation is using personal data, which should include for example: why it is using the data; what types of data will be used; how long the data will be kept for, and details of any transfers of data to third parties;
- The right to have access to a copy of the personal data that an organisation holds (known as a subject access request);
- The right to challenge the accuracy of personal data, and to ask for it to be corrected or deleted;
- In some circumstances, the right to have all personal data held erased (the right to be forgotten);
- The right to limit the way in which an organisation uses personal data;
- The right to have the personal data in a way that is accessible and machine readable (for example as a comma separated values (csv) file in Microsoft Excel). This is known as the right to data portability, and
- The right to object to the use of personal data, this includes an absolute right to object to personal data being used for direct marketing.

Individuals who may have concerns about an organisation's information rights practices have the right to make a request to the ICO for an assessment to be made to determine whether any provision of data protection law has been contravened.

2.5 Disclosure

Disclosure of personal information is governed by the first and second principles of the DPA concerning 'processing'. Some examples where disclosure of personal health data might be considered are:

- A legal duty requiring health and adult social care bodies to share information with each other for the direct care of a patient.
- Administration (e.g. to recover payment for treatment or for audit purposes to improve efficiency).
- Research & teaching (e.g. statutory or non-statutory disclosures to disease registries and for epidemiological research, clinical trials, or teaching).
- Non-health purposes (e.g. disclosures for Crime and Disorder Act 1998 (Ref 6) purposes, to the police, to hospital chaplains, or to the media).

For a person's direct care, the default position should be to share unless there is a reason not to. The Health and Social Care (Safety and Quality) Act (Ref 7) aims to address the 'culture of anxiety' with regards to data sharing that was identified by the 2013 Caldicott Report (Ref 8).

Use of the hospital or National Health Service (NHS) number rather than patient name, and encryption and anonymisation of data are recommended where appropriate.

Consent is not required where there is a risk of harm or abuse to the data subject or other people, where a serious crime is being investigated, or where there is a legal duty or requirement (see Section 3.6 - Exemptions).

For further information, particularly regarding specific requests for disclosure please refer to the Trust's Information Governance Policy (Ref 9).

2.6 Exemptions Allowing Disclosure

Exemptions vary according to the particular circumstance and range from total exemption from the principles, notification, and data subject access, to more limited exemption. There are a number of exemptions to the full operation of the DPA 2018, but they are limited to certain circumstances.

Exemptions are complex and should be used with care. The Data Protection Officer / IG Team can provide assistance and guidance if an exemption is to be considered. Some examples of exemption are:

- To safeguard national security;
- To enable the prevention and detection of crime and the apprehension or prosecution of offenders;
- Disclosures required by law or in connection with legal proceedings;
- Information for the discharge of a regulatory activity, such as protecting members of the public against dishonesty, malpractice or seriously improper conduct of professional persons, or for securing the health, safety and welfare of persons at work; and,
- To prevent prejudice to the combat effectiveness of the armed forces.

2.7 Subject Access Requests

To gain access to their personal data, an individual, usually a patient or employee, must apply in writing to the holder of that data (in this case the Trust). These requests are known as Subject Access Requests (SARs).

Following receipt of a subject access request, the information requested must be provided promptly and where possible within 21 calendar days, as advised by the Department of Health and Social Care. However, the legal requirement under data protection law is to respond within one calendar month.

All subject access requests must be logged by the relevant department or team and response times monitored. The Health Records Manager will provide a quarterly report to the Information Governance Steering Group (IGSG). All requests must be logged directly onto the Trust's Request for Information (RFI) system or notified by email to the Health Records Manager.

2.7.1 Health Records

For further details about access to health records, please refer to the Trust's Health Records Subject Access Requests Procedure (Ref 10).

2.7.2 Non-Health Records

Subject access requests may also be made for non-health records, for example, employment records and complaint files. Comprehensive guidance regarding subject access for employees is provided by the ICO in The Employment Practices Code and The Employment Practices Code Supplementary Guidance (Ref. 11). The following is an extract from that guidance:

Examples of personal information concerning employees likely to be covered by the DPA include:

- Details of an employee's salary and bank account held on an organisation's computer system.
- An email about an incident involving a named employee.
- A supervisor's notebook containing information on an employee where there is an intention to put that information in that employee's personnel file.
- An individual employee's personnel file.
- Records of leave such as annual and/or sick leave taken by the employee.

A request for subject access to employment records is to be made in writing or using the form available from the intranet.

2.7.3 Access to Email

Requesters are entitled, under subject access rights, to copies of information held in emails that is about them. For information to fall within the DPA's subject access provisions the requester must be the subject of the information and the information must affect the requester's privacy. This means, in a staff request for example, that an email about an employee's conduct or performance must be provided. However, an email that only contains an employee's name on the email's address list need not be provided.

The Trust, will check wherever there is some likelihood that messages might exist, and will take into account any details the requester has provided to assist the Trust in locating the information about them. The standard practice will be to conduct manual searches in the relevant mailboxes using the requester's name to conduct the search. The IG Team may assist with any searches required as part of a subject access request, but do not have access to staff email accounts; therefore, these searches must be done by the owner of the email account.

2.7.4 Third Party Information

Information that identifies another person, for example a work colleague, is known as third party information. Release of this information could lead to the third party's rights under the DPA being infringed. In many cases, simply removing the third party name from the information before it is disclosed will resolve the problem. However, a requester may be able to work out the identity of the

third party from the information itself. The Trust has to strike a balance between the right of the requester to access the information and the right of the third party to privacy. A clear and documented decision-making process is to be followed before releasing any such information.

2.7.5 Closed-Circuit Television (CCTV) Images

CCTV used on Trust premises is primarily for protection of patients, staff and visitors, preventing or detecting crime, and security purposes. The ICO guidance (Ref 12) confirms that most uses of CCTV by organisations or businesses will be covered by the DPA and therefore individuals whose images are recorded have a right to view the images of themselves and, subject to respecting the privacy of other data subjects in the images, to be provided with a copy of the images.

In terms of the data held on the CCTV system, the Trust is the data controller and the Facilities Service provider (Serco) is the data processor. Subject access requests for CCTV images at the Great Western Hospital (GWH) should be made through the Patient Advice and Liaison Service (PALS) or directly to the data processor (Serco).

Subject access requests for CCTV images at community sites should be made through Facilities Management.

For further information please refer to the CCTV Code of Practice (Ref. 12) published by the Information Commissioner's Office.

2.7.6 Charges for Subject Access Requests

In accordance with data protection legislation most requests for copies of records will not incur a charge. However, a reasonable fee can be charged for further copies of the same information or when a request is manifestly unfounded or excessive, particularly if it is repetitive. Any fee will be based on the administrative charge of providing the information. Further details of fees can be found in the Trust's Health Records Subject Access Procedure (Ref 10).

2.8 Data Controller Register

From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader who processes personal information to register as a data controller to pay a data protection fee to the ICO, unless they are exempt. There is a three tier scale for the fee which must be paid.

The Trust, as a public authority must pay a fee of £2,900 per annum and must register details of its Data Protection Officer.

The process by which details are added to the register of fee payers is the responsibility of the Data Protection Officer. The ICO maintains a public register of data controllers who are fee payers.

Data controllers who pay the data protection fee are listed on the data protection register, which is available from the ICO's website. The information published on the register is limited to:

- The name and address of the controller, but not details about individuals nominated as contact points for the ICO;
- The organisation's data protection registration number;
- The level of fee paid;
- The date the fee was paid and when it is due to expire;

- Any other trading names used;
- Contact details for the DPO, and the name of your DPO, if they consent to this being published.

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	Monitoring or audit method	Monitoring responsibility (individual, group or committee)	Frequency of monitoring	Reporting arrangements (committee or group the monitoring results is presented to)	What action will be taken if gaps are identified
Assessment of Trust performance and evidence against Data Protection & Security Toolkit assertions	On-line assessment	IG Team	Annually	IGSG and ARAC	Detailed action plan maintained by the IG Team for each year's assessment
Review of Subject Access Requests	Summary report of statistics and trends	Health Records Manager	Quarterly	Information Governance Steering Group	IGSG action plan for remedial work required
Annual renewal of data controller registration	Reminder sent from the ICO and renewal checked by the IG Team	IG Team	Annually	Information Governance Steering Group	Reminder to the Data Protection Officer
Annual Data Flow Mapping Exercise	Assessment tool and summary report approved by Senior Information Risk Owner (SIRO)	IG Team	Annually	Information Governance Steering Group – final approval by SIRO	IGSG action plan for remedial work required
Information Asset / System Security Assessments	Assessment tool and summary report approved by SIRO	IG Team	Annually	Information Governance Steering Group – final approval by SIRO	IGSG action plan for remedial work required
Data Protection Impact Assessments	DPIA screening tool and/or full assessment completed for new projects	IG Team – Caldicott log	Quarterly	Information Governance Steering Group	IGSG action plan for remedial work required

Review of incidents	Safeguard system and DSPT incident reporting tool	IG Team	Annually	Information Governance Steering Group	IGSG action plan for remedial work required

4 Duties and Responsibilities of Individuals and Groups

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non Clinical Services

All Ward Managers, Matrons and Managers for Non Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.4 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Trust has nominated the Medical Director to act as Caldicott Guardian and the Deputy Medical Director to act as Deputy Caldicott Guardian.

4.5 Senior Information Risk Owner (SIRO)

The Trust is required to nominate an employee of Board level to be accountable for the organisation's information risk. The Trust has nominated the Director of Finance to act as SIRO and the Deputy Director of Finance to act as Deputy SIRO.

4.6 Data Protection Officer

The Data Protection Officer will assist the Trust to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (the ICO).

4.7 The Information Governance Steering Group (IGSG)

The Information Governance Steering Group is responsible for overseeing all aspects of data protection alongside other initiatives and work areas, including freedom of information and information security management.

4.8 Information Asset Owners (IAOs) / Information Asset Administrators (IAAs)

Senior managers who are accountable for systems, known as Information Asset Owners (IAOs) and employees with delegated authority to manage the system, known as Information Asset Administrators (IAAs) have a responsibility to complete an annual information asset security assessment.

4.9 All Employees

It is everyone's responsibility to ensure they comply with this policy, with special regard given to the Data Protection principles. Data subjects, whether patients, carers, employees, their family or friends, all have a right of privacy and this policy aims to establish data protection by default.

5 Further Reading, Consultation and Glossary

5.1 References, Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) which employees should refer to for further details:

Ref. No.	Document Title	Document Location
1	Trust Privacy Notices	Trust Internet website
2	General Data Protection Regulation (EU) 2016/679	https://eur-lex.europa.eu
3	Data Protection Act 2018	www.legislation.gov.uk
4	Human Rights Act 1998	www.legislation.gov.uk
5	Freedom of Information Act 2000	www.legislation.gov.uk
6	Crime and Disorder Act 1998	www.legislation.gov.uk
7	Health and Social Care (Safety & Quality) Act 2015	www.legislation.gov.uk
8	Caldicott Principles	www.gov.uk/government
9	Information Governance Policy	T:\Trust-wide Documents
10	Subject Access Requests Procedure	T:\Trust-wide Documents
11	Employment Practices Code & Supplementary Guidance	www.ico.org.uk
12	CCTV Code of Practice	www.ico.org.uk
13	European Union (Withdrawal) Act 2018	www.legislation.gov.uk

5.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department.	Date Consultee Agreed Document Contents
Senior IG Officer	4 June 2021

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and can be found at Appendix A.

Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project? Data Protection Policy		
2.	Briefly describe the aim of the policy, strategy, and project. What needs or duty is it designed to meet? This document provides clear guidance concerning data protection within the Trust, and describes the legal obligations and responsibilities for the Trust as a whole, and for individual employees. It also describes the process necessary to renew the Trust's Data Protection registration, identifies responsible persons, and describes the Trust's purposes for processing personal information.		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?		**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?		**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?		**No**

Signed by the manager undertaking the assessment	M Arnold
Date completed	07 July 21
Job Title	Head of Information Governance and DPO

On completion of Stage 1 required if you have answered YES to one or more of questions 3, 4 and 5 above you need to complete a STAGE 2 - Full Equality Impact Assessment

Equality Impact Assessment

Are we Treating Everyone Equally?

Define the document. What is the document about? What outcomes are expected?

Consider if your document/proposal affects any persons (Patients, Employees, Carers, Visitors, Volunteers and Members) with protected characteristics? Back up your considerations by local or national data, service information, audits, complaints and compliments, Friends & Family Test results, Staff Survey, etc.

If an adverse impact is identified what can be done to change this? Are there any barriers? Focus on outcomes and improvements. Plan and create actions that will mitigate against any identified inequalities.

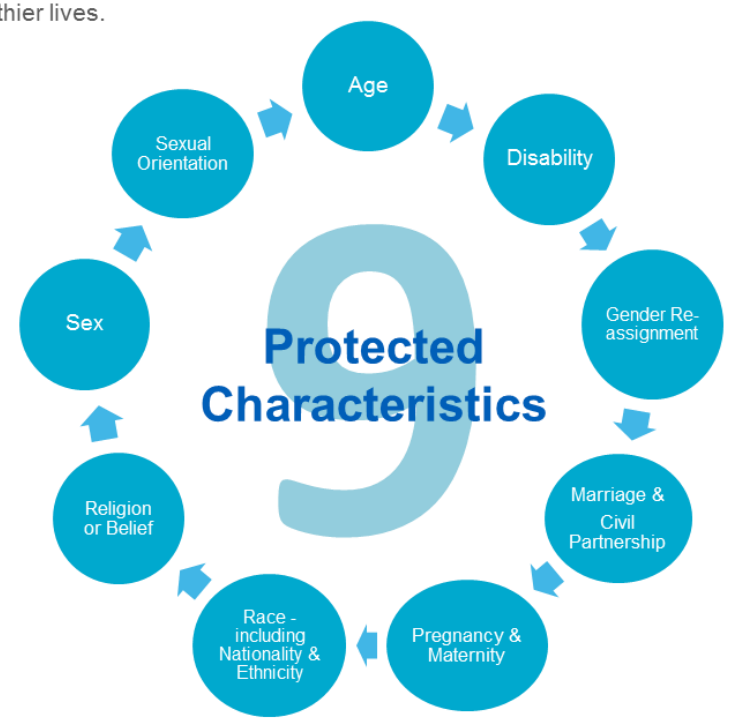
If the document upon assessment is identified as having a positive impact, how can this be shared to maximise the benefits universally?

Trust Equality and Diversity Objectives

Better health outcomes for all	Improved patient access & experience	Empowered engaged & included staff	Inclusive leadership at all levels

Our Vision

Working together with our partners in health and social care, we will deliver accessible, personalised and integrated services for local people whether at home, in the community or in hospital empowering people to lead independent and healthier lives.



Appendix B – Lawful Basis for Processing Information Flowchart