Barnet, Enfield and Haringey NHS
Mental Health NHS Trust

Data Protection Policy

Version:	5
Policy Number:	IG 05
Policy Lead/Author & Position:	Chief Information Officer
Responsible Directorate:	Information Governance
Replacing Document:	Data Protection Policy v4
Approving Committee / Group:	Information Governance Group
Date Approved/Ratified:	
Ratified by:	Policy Development Monitoring Review Group
Previous Reviewed Dates:	Jan 2006, Jan 2009, June 2012, July 2014, 2017
Date of Current Review:	September 2021
Date of Next Review:	September 2023
Relevant NHSLA Standard CQC Outcome(s):	
Target Audience	All staff

EQUALITY STATEMENT

Barnet, Enfield and Haringey NHS Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Equality Act (2010) including the Human Rights Act 1998 and promotes equal opportunities for all.

This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.
Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Barnet, Enfield and Haringey NHS Trust embraces the four staff pledges in the NHS Constitution and this policy is consistent with these pledges.

Version Control Summary

Version	Date	Section	Author	Comments
2	19.06.12	All sections	Director of Strategy & Performance	All sections reviewed in line with NHSLA requirements
3	30.07.15	Various sections	Information Governance Manager	Changes to accountabilities, updated Caldicott Principles, reference to Connecting for Health removed, updated TOR, added process for managing subject access requests.
4	29.12.17		Data Protection Officer	Amended to meet GDPR requirements
5	04/10/2021	Various sections	Information Governance	Updated Caldicott Principles Removed reference to Registration Authority policy (Document obsolete)

Contents

1 Policy Statement

The Data Protection Policy outlines the Trust's protocols and procedures regarding the implementation, maintenance and observance of Data Protection strategies within the organisation, in line with the requirements of current Data Protection legislation including the General Data Protection Regulation (GDPR).

2 Introduction

Principally, the Policy recognises that the ultimate objective of Data Protection legislation is to regulate the ways in which personal information about individuals (be it staff, patients or visitors) is obtained, stored (whether within electronic records or a manual filing systems), used and disclosed. Furthermore, the Policy acknowledges that the legislation grants certain rights to individuals, enabling them to have access the data stored about them, and if it is incorrect, to either apply for modification of the data.

- The Trust shall fully support and comply with the principles of the DPA of 2018. This act covers "personal data" which can be used to identify a living individual.
- The DPA 2018 applies the standards set out in the EU General Data Protection Regulation (GDPR) but has been amended to reflect the national context[1] and is now known as UK GDPR. The DPA 2018 updates and replaces the DPA of 1998 and came into effect on 25 May 2018.

- The Trust shall register annually with the Information Commissioner's Office (ICO). This is a requirement placed upon the Trust as a body that manages and processes personal data.

3 Purpose and Aim

The purpose and aim of this policy is to ensure the Trust adopt procedures to minimise the risk of breaching data protection legislation.

4 Scope and Outcome

The GDPR presents a number of significant challenges. Not only must the Trust ensure their appreciation of, and respect for basic Data Protection objectives, but they must also comply with all the specifics contained within the legislation. Some of the most far-reaching of these specifics come as a result of guidance contained within the GDPR and Data Protection Act of 2018. The Trust must, at all times, be able to provide a lawful basis for the processing of personal data and must ensure that all processing of high risk personal data is notified to the Information Commissioners Office.

This Policy entails all personal data held by, or on behalf of, the Trust, its processing, storage, handling and usage. Such data includes but is not limited to:

- employee and staff records;
- patient data and records;
- personal data relating to volunteers working with the Trust;
- personal data in all formats including, but not limited to, paper copy, digital records and CCTV.

Are used and processed in accordance with Data Protection legislation.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

This Policy applies to all those working for the Trust in whatever capacity, including the Trust's staff, volunteers, students, temporary workers, contractors, suppliers and Third Parties (hereafter referred to as 'Employees'). It applies to Third Party providers who may hold Information belonging to the Trust, including patient information. Suppliers are also expected to follow this approach as part of their own obligations under the DPA 2018.

5 Definitions

Data Protection Act (2018)

The DPA 2018 stipulates that anyone processing personal data must comply with the following principles[2], in which personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ("fair, lawful and transparent");
- 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 not be considered to be incompatible with the initial ("purpose limitation");
- used in a way that is adequate, relevant and limited to only what is necessary ("data minimisation");
- accurate and, where necessary, kept up-to-date ("accuracy");
- kept for no longer than is necessary ("storage limitation");
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage ("confidentiality and integrity").

The Legislation stipulates that there shall be accountability which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. There must also be appropriate measures and records in place to be able to demonstrate compliance.

The DPA 2018 provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data [3].

Although the DPA 2018 does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be afforded to the records and information relating to a deceased person as applies to a living person.

Personal data – The GDPR defines 'personal data' as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive personal data - The GDPR refers to sensitive personal data as "special categories of

[2] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[3] For definitions, refer to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

personal data" and includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Processing - includes obtaining, recording, holding, obtaining, sharing, using the information or data or carrying out any operation or set of operations on the information or data.

Data Subject – " a living individual who is the subject of the personal data".

Data Controller - 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.

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Third party – in relation to personal data, means any person other than –

(a) The data subject,

(b) The data controller, or

(c) Any data processor

Consent – in accordance with the GDPR consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. Records to demonstrate consent must be kept.

Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help organisations identify and minimise the data protection risks of a project.[4]

Employees shall complete a DPIA when seeking to process information that is likely to result in a high risk to individuals. To assess the level of risk, both the severity and likelihood of any impact to an individual/s should be considered.

The Employee should ask the Data Protection Officer (DPO) for their advice on the DPIA and document it as part of the process.

Privacy Notice and Fair Processing

The EU GDPR requires that data controllers provide certain information to people whose data they hold and use.[5] This is known as a Privacy Notice (PN).

The Trust shall provide PNs to all patients and all Employees, identifying who the data controller is, including contact details for the DPO. The PN should also explain the purposes for which personal data is collected and used, how the data is used and disclosed, how long it is kept, and the controller's legal basis for processing.

[4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
[5] https://ico.org.uk/global/privacy-notice/

A Statement of Fair Processing / Privacy Notice should also be provided on the Trust's website. This reflects the requirement for a Statement of Fair Processing set out in the recommendations of the Caldicott Review.

NHS Caldicott Principles

The Trust shall also comply with the Caldicott Principles which focus on the protection and processing of patient-identifiable information within the NHS.
The Caldicott Guardian has been appointed by the Trust to advise the Trust Board on the matter of patient confidentiality and promote safe and secure handling of patient data.

Network and Information Systems Regulation (NISR)

The Networks and Information Systems Regulation aims to raise the levels of overall security and resilience of network and information systems for Operators of Essential Services across the UK and defines a set of principles used to guide decision-making. These principles fall under four main objectives:

- **Managing the Security Risks**: by ensuring appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services;
- **Protecting Against Cyber Attacks**: by ensuring proportionate security measures are in place to protect essential services and systems from Cyber-attack;
- **Detecting Cyber Security Events**: by ensuring security defences remain effective and detecting Cyber Security events affecting, or with the potential to affect, essential services;
- **Response and Recovery Planning**: having capabilities to minimise the impact of a Cyber Security incident on the delivery of essential services including the restoration of those services where necessary.

NHS Code of Practice

Under the NHS Code of Practice, individuals have a right to confidentiality. Further guidance regarding confidentiality can be found in the NHS Code of Conduct. Please refer to the 'NHS Code of Practice for Confidential Information' for further detail[6].

Freedom of Information Act 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities;
- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Public authorities include government departments, local authorities, the NHS, state schools and police forces.

[6] https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that the Trust holds about them, they should make a Subject Access Request under the Data Protection Act.

6 Duties

The following key roles are responsible for data protection regulations in the Trust.

6.1. Chief Executive and the Trust's Board

Have ultimate accountability for actions and inactions in relation to this Policy. The Board is responsible for ensuring that Data Protection legislation is addressed at the strategic level.

6.2. Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. They ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

6.3. Caldicott Guardian

Has overall responsibility for ensuring all information related to patients and users of the service that the Information Commissioner regulates, is used confidentially and handled with appropriate safeguards

6.4. Data Protection Officer

Data Protection Officer (DPO) is accountable to the Chief Information Officer. The role of the DPO is to inform and advise the Trust and its employees about their obligations to comply with data protection laws. The DPO will be the first point of contact for supervisory authorities such as the Information Commissioner and for individuals whose data is processed (employees, customers etc).

6.5. Managers

All managers are responsible for ensuring the staff that they manager are aware and familiar with this policy, either through local induction and/or one to one supervision meetings. Managers are also responsible for ensuring that staff within their respective areas of management are aware of their responsibilities in relation to providing staff with information aligned to the standards of Data Protection legislation.

6.6. Employees

All Trust employees are personally responsible for ensuring they comply with this policy

6.7. Information Governance Group

Has overall responsibility for ensuring that systems and processes are in place to drive the information governance agenda and strategy, and to support the implementation and development of Information Governance and Data Protection. See Terms of Reference for details and membership.

7 Caldicott Principles

The Caldicott Report of 1997 established a number of general principles that health and social

care organisations should use when reviewing its use of client information. Since then the principles have been updated, following further reports in 2013 and 2020. The Caldicott Standards are based on Data Protection legislation. The 8 Caldicott principles are shown below:

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

These eight principles, which are broadly similar to those contained in Data Protection legislation, apply to all employers and their employees. Articles 6 and 9 of the GDPR provide further conditions for processing data.

Article 5 of the GDPR requires that personal data shall be

1. Processed fairly and lawfully and, in particular, shall not be processed unless: one of the conditions in Article 6 is met; in the case of sensitive personal data, at least one of the

conditions in Article 9 is also met. – ***see Appendix One***.)

2. 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 not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. 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.
5. 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.

Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with these principles."

Individual Rights

The GDPR identifies individual's' rights as:

1. The right to be informed - emphasises the need for transparency over how the Trust uses personal data
2. The right of access - Individuals have the right to access their personal data and supplementary information, timescales apply.
3. The right to rectification - Personal data can be rectified if it is inaccurate or incomplete.
4. The right to erase - enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5. The right to restrict processing – under certain circumstances individuals have a right to 'block' or suppress processing of personal data
6. The right to data portability - allows individuals to obtain and reuse their personal data for their own purposes across different services, (conditions apply).
7. The right to object – includes the right to object to processing for purposes of scientific/historical research and statistics
8. Rights in relation to automated decision making and profiling.

Detailed information on individual's rights is available on the Information Commissioners website

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

9. Rights of Subject Access

Under the terms of the GDPR a data subject maintains certain rights regarding access to any personal information about them held by the Trust, whether in an electronic or manual format.

A data subject may request notification from a Data Controller in relation to:

- whether personal data about the individual is being processed.

- the nature of the data, the purpose or purposes for which it is being processed and
- the recipients or classes of recipient to whom it is, or may be, disclosed.
- the content of the data, to be communicated back to the data subject in writing within one month together with any relevant information as to the source of the data.
- the logic involved in any computer assisted decision making.

See Trust Subject Access Request policy available on the Intranet for detailed information

10. Rights of Subject Access

In accordance with the GDPR a data controller must have a valid lawful basis in order to process personal data. The conditions for lawful processing are shown in appendix 2.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis. You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.

11. Associated Trust Documents

Information Sharing Policy Information Security Policy Data Quality Policy
Information Governance Strategy Information Risk Policy
Records Management and Information Life Cycle Policy
Information Governance Incident Management Policy Consent to Treatment Policy
Subject Access Request Policy

Available on the Trust Intranet - Policies and procedures

12. Monitoring Compliance and Effectiveness

The Information Governance group will monitor these procedures to ensure that users are adhering to them and to ensure they are kept up to date with new legislation.

In the event of a suspected breach of these procedures, the Trust may initiate further measures, such as disciplinary procedures.

13. Dissemination and Implementation

This document will be made available to all staff on the Trust Intranet and through line management cascade and brought to the attention of new staff via the induction process.

13.1. Training

Data Protection legislation requires all individuals who access personal data to receive Data Security Protection training, on an annual basis.

Evidence of training must be kept in the individual's personnel file. Data Protection training is included in the Trust's annual mandatory training plan. All staff are required to undertake training online e- learning via the Trust ESR training platform or an alternative approved method of learning.

14. Contributors

- Information Governance Manager & Data Protection Officer
- Information Governance Group

15. References

This policy has been prepared in reference to the documents listed below and should be read in conjunction with them, and are available on the Trust intranet

http://staff.beh-mht.nhs.uk/

- General Data Protection Regulation (GDPR)
- Caldicott principles
- Data Protection Act 2018
- Department of Health: Confidentiality NHS Code of Practice
- Department of Health: Information Security Management Code of Practice
- European Data Protection Directive
- Department of Health 2013: Information Governance Review– To Share or Not to Share, Caldicott 2
- National Data Guardian 2020: Response to consultation about Caldicott Principles and Guardians

Appendix one: Conditions for Processing Data

	Personal data – Article 6		Special Categories data (sensitive) – Article 9
1	The data subject has given consent to the processing	1	The data subject has given explicit consent to the processing
2	Contractual necessity – the processing is necessary • For the performance of a contract to which the data subject is a party or • For the taking of steps at the request of the data subject with a view to entering into a contract	2	Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
3	Non-contractual legal obligations of the Data Controller	3	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
4	To protect the vital interests of the data subject	4	The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject
5	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	5	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
6	Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	6	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
		7	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
		8	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
		9	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

16. MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF PROCEDURAL DOCUMENTS FORM

1.	**How will the document be monitored? (please circle as appropriate)**	**Audit**		**Review**	**Other, please specify;**
		Methodology:			
2.	**What is the process for reviewing results of monitoring?**	Discuss at IG Group			
3	**Report to:**	**SIRO**			
4.	**Who is responsible for conducting the monitoring? (please circle as appropriate)**	**Group / Committee**		**Individual**	
		Name / Title (also include position of individuals): IG Group			
5.	**How often will the document be monitored? (please circle as appropriate)**	**Monthly**	**6 Monthly**	**Yearly**	**Every 3 years**
		Comments: To be reviewed every 3 years or changes in legislation			
6	**Responsibility for action planning after review**				

17. EQUALITY IMPACT ASSESSMENT AND ANALYSIS FORM

1. Please indicate the expected impact of your proposal on people with protected characteristics					
Characteristics (where relevant)	Significant +ve	Some +ve	Neutral	Some -ve	Significant -ve
Age:		√			
Disability:		√			
Ethnicity:		√			
Gender re-assignment:		√			
Religion/Belief:		√			
Sex (male or female)		√			
Sexual Orientation:		√			
Marriage and civil partnership		√			
Pregnancy and maternity			√		
The Trust is also concerned about key disadvantaged groups event though they are not protected by law					
Substance mis-users			√		
The homeless			√		
The unemployed			√		
Part-time staff			√		
Please remember just because a policy or initiative applies to all, does not mean it will have an equal impact on all.					

2. Consideration of available data, research and information. (delete grey guidance text once read)

Please list any monitoring, demographic or service data or other information you have used to help you analyse whether you are delivering a fair and equitable service. Social factors are significant determinants of health or employment outcomes. Monitoring data and other information should be used to help you analyse whether you are delivering a fair and equitable service. Social factors are significant determinants of health outcomes. Please consult these types of potential sources as appropriate. There are links on the Trust website:

- Joint strategic needs analysis (JSNA) for each borough
- Demographic data and other statistics, including census findings
- Recent research findings (local and national)
- Results from consultation or engagement you have undertaken
- Service user monitoring data (including age, disability, ethnicity, gender, religion/belief, sexual orientation and)
- Information from relevant groups or agencies, for example trade unions and voluntary/community organisations
- Analysis of records of enquiries about your service, or complaints or compliments about them
- Recommendations of external inspections or audit reports

	Key questions (supports EDS Goals)	Your Response *Please reference data, research and information that you have reviewed which you have used to form your response*
2.1	What evidence, data or information have you considered to determine how this development contributes to delivering better health outcomes for all?	Policy is made in accordance with NHS Digital's Code of Practice on Confidential Information Records Management Code of Practice
2.2	What evidence, data or information have you considered to determine how this development contributes to improving patient access and experience?	Gender Recognition Act 2004 http://www.legislation.gov.uk/ukpga/2004/7/contents

2.3	What evidence, data or information have you considered to determine how this change/development/plan/policy contributes to delivering a representative and well supported workforce?	NHS Digital's Code of Practice on Confidential Information https://digital.nhs.uk/information-governance
2.4	What evidence, data or information have you considered to determine how this change/development/plan contributes to inclusive leadership and governance?	Information Commissioner's office website https://ico.org.uk/

3. It is Trust policy that you explain your proposed development or change to people who might be affected by it, or their representatives. Please outline how you plan to do this.

Group	**Methods of engagement**

4. Equality Impact Analysis Improvement Plan

If your analysis indicates some negative impacts, please list actions that you plan to take as a result of this analysis to reduce those impacts, or rebalance opportunities. These actions should be based upon the analysis of data and engagement, any gaps in the data you have identified, and any steps you will be taking to address any negative impacts or remove barriers. The actions need to be built into your service planning framework. Actions and targets should be measurable, achievable, realistic and time framed.

Negative impacts identified	Actions planned	By who

6. Sign off and publishing

Once you have completed this form, it needs to be 'approved' by your Service Director, Clinical Director or an Executive Director or their nominated deputy. If this Equality Impact Analysis relates to a policy, procedure or protocol, please attach it to the policy and process it through the normal approval process. Following this sign off by the Clinical Policy Working Group (clinical policies only) or Executive lead group for non-clinical policies your policy and the associated EqIAn will be published by on the intranet. If your EqIAn related to a service development, business plan, financial plan or strategy, once your Director or the relevant committee has approved it please send a copy to the Equalities Team (beh-tr.equalities@nhs.net), who will publish it on the Trust's intranet. Keep a copy for your own records.	
I have conducted this equality Impact analysis in line with Trust guidance	
Your name: Mary Olubi	Position: Information Governance Manager
Signed: MOlubi	Date: 07/10/2021
Approved by:	
Your name:	Position
Sign:	
Date	

Checklist for the Review and Approval of procedural Document
To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**	**Data Protection Policy**	
	Is the title simple and clear to everyone who reads it?	**Yes**	
	Is it clear whether the document is a guideline, policy, protocol or standard?	**Yes**	
2.	**Rationale**		
	Are reasons for development of the document stated?	**Yes**	
3.	**Development Process**		
	Is the method described in brief?	**Yes**	
	Are individuals involved in the development identified?	**Yes**	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	**Yes**	
	Is there evidence of consultation with stakeholders and users?	**Yes**	
4.	**Content**		
	Is the objective of the document clear?	**Yes**	
	Is the target population clear and unambiguous?	**Yes**	
	Are the intended outcomes described?	**Yes**	
	Are the statements clear and unambiguous?	**Yes**	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	**Yes**	
	Are key references cited?	**Yes**	
	Are the references cited in full?	**Yes**	
	Are local/organisational supporting documents referenced?	**Yes**	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	**Yes**	
	If appropriate, have the joint staff side committee (or equivalent) approved the document?	**Yes**	
7.	**Dissemination and Implementation**		

	Is there an outline/plan to identify how this will be done?	**Yes**	
	Does the plan include the necessary training/support to ensure compliance?	**Yes**	
8.	**Document Control**		
	Does the document identify where it will be stored?	**Yes**	
	Have archiving arrangements for superseded documents been addressed?	**Yes**	
9.	**Process for Monitoring Compliance**		
	Are there measurable standard to support monitoring compliance of the document?	**Yes**	
	Is there a plan to review or audit compliance with the document?	**Yes**	
10.	**Review Date**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Is the review date identified?	**Yes**	
	Is the frequency of review identified? If so, is it acceptable?	**Yes**	
11.	**Overall Responsibility for the Document**	**Yes**	**Information Governance Team**
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	**Yes**	