Data Protection Policy

Controlled document
This document is uncontrolled when downloaded or printed.

Reference number	WHHT: G022
Document type	Policy
Version	8
Author's name & job title	Nicola Bateman, Information Governance and Data Protection Manager
Department/Speciality	Information Governance
Division	Business Support
Reviewed by	Informatics Group
Review date	05/02/2021
Approved by PGRG	Feb 2021
Ratified by QSG	March 2021
Next review date	February 2024
Target audience	All staff
Search terms	Data Protection, Confidentiality, Information Governance
Previous document name (if different)	Data Protection 2018 Policy

CONTRIBUTION LIST
Key individuals involved in developing this version of the document

Name	Designation
Nicola Bateman	Data Protection Officer and Information Governance Manager

Change History

Version	Date	Author	Reason for change
1	April 07	Nicola Bateman	Policy approved.
2	June 09	Nicola Bateman	Included section on Confidentiality & Monitoring & Review. Updated section on Responsibilities. Further minor changes made throughout the policy.
3	Feb 10	Nicola Bateman	Recommendations from Information Commissioners Office incorporated into the policy document.
3	May 12	Nicola Bateman	Minor amendments -
4	July 12	Nicola Bateman	Full update as policy due to expire
5	Aug 2014	Nicola Bateman	Review – minor amendments and additions
6	Sep 16	Nicola Bateman	Section of Safe Harbour has been removed as this has been replaced with the EU-US Privacy Shield as from 1st Aug 2016. Minor additions and amendments regarding policy names and hyperlinks. Research & Development Section amended to reflect new process for undertaking clinical research within the Trust.
7	Sep 18	Nicola Bateman	Updated to incorporate new data protection laws including GDPR and DPA18
8	Jan 21	Nicola Bateman	Updated to incorporate changes from the UK leaving the EU. Data Protection 2018 Act now supplements/sits alongside the EU GDPR. Other additional minor amendments.

Abbreviations and Acronyms

Abbreviations and Acronyms	Description
MDT	Multidisciplinary Team
PGRG	Policy & Guideline Review Group
QSG	Quality & Safety Group

CONTENTS

1 Introduction

West Hertfordshire NHS Hospitals Trust (the Trust) is committed to ensuring the privacy of individuals are respected and that all Personal Data processed is handled appropriately and in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) collectively known in this policy document as (Data Protection Legislation).

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR.

The UK GDPR is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of Personal Data in the UK, except for law enforcement and intelligence agencies.
It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The Trust has a legal obligation to comply with all appropriate legislation and guidance when processing Personal Data about patients, employees and all other identifiable individuals.

2 Objectives

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

- observe fully conditions regarding the fair and lawful collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information to the extent that it is needed to fulfil operational needs or to comply with legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under UK Data Protection Legislation.
- take appropriate technical and organisational security measures to safeguard personal information;

3 Definitions

Data Protection Legislation refers to both the UK General Data Protection Regulations (2018) and the Data Protection 2018 Act. The following definitions apply.

Personal Data means 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Special Category Data consists of Personal Data relating to: - ethnic origin, - physical and mental health (including, for example, details of the reasons for an individual's sick leave), - sex life, - genetics - biometrics (where used for ID purposes) - religion or belief, - political opinion - Trade Union membership Greater protections are required when processing this data.

Processing means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data. Data Subject "Data Subject" means an individual who is the subject of the Personal Data.

Data Controller means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any Personal Data is processed. In this case, this means the Trust or nominated individuals acting on behalf of and with the authority of the Trust.

Data Processor means any person (other than a member of staff) or organisation that processes data on behalf of the Trust.

4 Scope

This policy must be followed by all staff working for or on behalf of the Trust, including those on temporary or honorary contracts, secondments, volunteers, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services.

The policy is applicable to all areas of the Trust and covers all aspects of information including (but not limited to):

- Patient/Client/Service User information.
- Personnel/Staff information.
- Organisational and business sensitive information.
- Structured and unstructured record systems - paper and electronic.
- Photographic images, digital, text or video recordings including CCTV.
- All information systems purchased, developed and managed by/or on behalf of, the organisation.
- Information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information.
- Retrieval, consultation, storage/retention or use of information.
- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons.
- Alignment, combination/linkage, blocking, erasing or destruction of information.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

5 Responsibilities

5.1 Chief Executive

The Chief Executive holds overall responsibility for data protection throughout the Trust, but on a day-to-day basis will be delegated to the Data Protection Officer.

5.2 Senior Information Risk Owner (SIRO)

The Trust has appointed the Chief Information Officer as the Senior Information Risk Owner (SIRO).

The SIRO is responsible for:

- Acting as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of the Trust's statement of internal control in regard to information risk.
- Implementing and lead the NHS information governance risk assessment and management processes.
- Advising the Board on the effectiveness of information security risk management across the Trust.

5.3 Data Protection Officer (DPO)

The Information Governance Manger is the appointed Data Protection Officer (DPO). UK Data Protection Legislation specifies the following minimum duties or "tasks" to be performed by the DPO.

- To inform and advise the Trust, and their employees, of their obligations under the Regulation and other applicable laws and regulations.
- To monitor compliance with UK Data Protection Legislation and other applicable laws and regulations.
- To advise on Data Privacy Impact Assessments (DPIA) and monitor their performance, as required.
- To liaise with the Information Commissioners' Office (ICO) as required.
- To be the contact point for the general public.

5.4 Cyber Security Operations Manager

The Cyber Security Operations Manager is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes and shall:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for cyber security.

- Ensure the operational effectiveness of security controls and processes.
- Ensure that staff are aware of their responsibilities and accountability for cyber security.
- Be accountable to the SIRO and other bodies for Cyber Security across the Trust.
- Monitor potential and actual security breaches with appropriate expert security resource.

In carrying out these tasks the Cyber Security Operations Manager will work closely with the Chief Information Officer, Director of ICT, Head of ICT Technical Services and the Data Protection Officer.

5.5 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the 8 Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

5.6 Managers

Managers in all business areas are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties. Managers must always contact the Data Protection Officer if:

- they are unsure of the lawful basis which they are relying on to process Personal Data;
- they need to rely on consent for processing Personal Data;
- they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA);
- they plan to use Personal Data for purposes other than those for which it was originally collected;
- they plan to carry out activities involving automated processing including profiling or automated decision-making;
- they need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our contractors);
- they plan to share data with another organisation or person in a way which is new or could affect Data Subjects' rights.

5.7 All Staff

Everyone working for us or on our behalf is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of Personal Data and support us in complying with data protection legislation:

6 Principles

Data Protection Legislation sets out the following main principles for Data Controllers and Data Processors when processing Personal Data.

6.1 Lawfulness, Transparency and Fairness

Lawfulness

To process Personal Data and special category data lawfully, the Trust must identify a legal basis for each data processing activity.

An annual data mapping exercise is undertaken across the Trust which identifies all inbound and outbound flows of Personal Data and an appropriate lawful basis for each flow is identified and documented.

Transparency and Fairness

General information about how we process Personal Data as a regulator (referred to as “fair processing information”) is available on our website through privacy notices and other public-facing material.

These notices are also included in starter packs for all staff when they first join .

https://www.westhertshospitals.nhs.uk/patientinformation/documents/Patient_Privacy_Notice_v1.0.pdf

6.2 Purpose Limitation

The Trust has clearly identified and documented the purposes for processing and details of these purposes are included in our privacy notices which we make available to both patients and our staff. All purposes are reviewed on an annual basis.

6.3 Data Minimisation

The Trust will only collect Personal Data required for specified purposes and ensure it is periodically reviewed and deleted when no longer required.

6.4 Accuracy

The Trust will take reasonable steps to ensure the accuracy of Personal Data and will carefully consider any challenges to the accuracy of information. This will be achieved by ensuring:

- appropriate processes are in place to check the accuracy of data;
- any mistakes are clearly identified as a mistake;
- all records will identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts;
- any challenges to the accuracy of Personal Data will be carefully considered when complying with an individual’s right to rectification;

6.5 Storage limitation

We will ensure that Personal Data is not kept in an identifiable form for longer than is necessary. Because of our functions as a public authority, the Trust retains some Personal Data for long periods of time.

Details of all of our retention and disposal periods are set out in our Records Retention and Disposal Policy.

6.6 Confidentiality, Integrity and Availability

A key principle of Data Protection Legislation is that Personal Data must be processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'. This will be achieved by ensuring:

- An information security policy is in place and implemented across the Trust.
- Additional policies and controls are in place to enforce them.
- Information security risk shall be adequately managed and risk assessments on ICT systems and business processes shall be performed where appropriate.
- The requirements for confidentiality, integrity and availability for the Personal Data we process are understood.
- Appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store the Trust information.
- Encryption and pseudonymisation processes are in place where it is appropriate to do so.
- Access to Personal Data can be restored in the event of any incidents, such as by establishing an appropriate backup process.
- Regular testing is conducted and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Measures are implemented that adhere to an approved code of conduct or certification mechanism when necessary.
- All relevant information security requirements of the Trust shall be covered in agreements with any data processors, third-party partners or suppliers, and compliance against these is monitored.

6.7 Accountability

The Trust is **responsible** for complying with Data Protection Legislation and must be able to **demonstrate** compliance by evidencing the steps taken to comply. This will be achieved by ensuring:

- we take responsibility for complying with Data Protection Legislation, at the highest management level and throughout our organisation;

- we keep evidence of the steps we take to comply;

- appropriate technical and organisational measures are in place, which will be achieved by;

  - adopting and implementing data protection policies;
  - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
  - putting written contracts in place with organisations that process Personal Data on our behalf;
  - maintaining documentation of our processing activities;
  - implementing appropriate security measures;
  - recording and, where necessary, reporting Personal Data breaches;
  - carrying out Data Protection Impact Assessments (DPIA) for uses of Personal Data that are likely to result in high risk to individuals' interests;
  - appointing a data protection officer;
  - adhering to relevant codes of conduct and signing up to certification schemes (where possible);
  - We review and update our accountability measures at appropriate intervals.

7 Lawful basis for processing

The Trust will determine which lawful basis applies when processing Personal Data. These are set out as follows in Data Protection Legislation. At least one must be identified whenever Personal Data is processed:

(a) Consent: the individual has given clear consent to process their Personal Data for a specific purpose.

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

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(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 which overrides those legitimate interests. (This cannot apply when the Trust is processing data to perform its official tasks).

In order to process **Special Categories Data**, the Trust must also ensure that one of the following applies:

a) the Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection;

(c) processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

(e) processing relates to Personal Data which are manifestly made public by the Data Subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest;

(h) 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;

(i) 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

8 Consent

When relying on consent as the legal basis for lawful sharing of Personal Data, ensure the quality of consent meets new requirements and that:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
- consent to processing is distinguishable, clear, and is not *"bundled"* with other written agreements or declarations;
- Data Subjects are informed that they have the right to withdraw
- there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
- separate consents are obtained for distinct processing operations; and
- consent is not relied on where there is a clear imbalance between the Data Subject and the controller (especially if the controller is a public authority).

9 Individuals Rights

The Trust will respect individuals' rights when processing Personal Data. These are enshrined in Data Protection Legislation as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

The right to be informed is, however, a key right and applies in all circumstances (see Transparency above).

10 Contracts

When the Trust engages with a Supplier or Data Processor a written contract will be in place to ensure both parties understand their responsibilities and liabilities. Data Protection Legislation sets out what needs to be included in the contract.

Contracts will set out the subject matter, duration, nature and purpose of the processing, the type of Personal Data and categories of Data Subject, and the obligations and responsibilities of both parties which must, as a minimum set out the following:

- only act on the written instructions of the Trust;
- ensure that people processing Personal Data are subject to a Duty of Confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the Trust and under a written contract;
- assisting the Trust in compiling with Subject Access Requests;
- assisting the Trust in meeting its responsibilities in relation to the security of Personal Data;
- notifying the Trust of Personal Data breaches;
- assisting with completing Data Privacy Impact Assessments when necessary;
- delete or return all Personal Data to the controller as requested at the end of the contract;
- submit to audits and inspections as required.

The Trust will apply the approach set out in the Procurement Policy Note (PPN02/18) Changes to Data Protection Legislation & General Data Protection Regulation, published by Crown Commercial Service - https://www.gov.uk/government/publications/procurement-policy-note-0218-changes-to-data-protection-legislation-general-data-protection-regulation.

11 Record of Processing Activities

The Trust is required to maintain a record of its processing activities, covering areas such as processing purposes, data sharing and retention.

A Data Mapping review of all data processing activities across the Trust will be undertaken on an annual basis coordinated by the Information Governance team. The review will identify all inbound and outbound flows of personal identifiable information from each department and clinical area, the purposes of the flow, what type of Personal Data is involved, who it is shared with, the lawful basis and whether an information sharing agreement has been established.

12 Data Protection by Design and Default

The Trust will ensure that privacy and data protection issues are considered at the design phase of any new system, service, product or process and that appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights are in place. This will involve but not limited to;

- Only using Data Processors and Suppliers that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- Anticipating risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals
- Making data protection an essential component of the core functionality of our processing systems and services.

13 Data Privacy Impact Assessment (DPIA)

Data Protection Legislation introduces obligations to carry out a DPIA before carrying out types of processing likely to result in high risk to individuals' interests.

The Trust will consider if a full DPIA is necessary if the processing of Personal Data involves:

- evaluation or scoring (including profiling and predicting)
- automated decision making
- systematic monitoring of Data Subjects, including in a publicly accessible area
- sensitive data (special categories of data and data regarding criminal offences)
- data being processed on a large scale
- matched or combined datasets
- vulnerable individuals
- Innovative technological or organisational solutions
- preventing Data Subjects from exercising a right or using a service or a contract

As a minimum, a DPIA will include;

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of
  (i) the need for and proportionality of the processing and
  (ii) the risks to Data Subjects (as viewed from the perspective of Data Subjects) arising; and

- A list of the measures envisaged to mitigate those risks and ensure compliance with the Data Protection Legislation.
- A mechanism for updating the Trusts' records of internal data processing activities to ensure new data sharing initiatives are included – See Section 11 Record of Processing Activities.

14 Data Protection Officer

Data Protection Legislation introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

The Trust's DPO is Nicola Bateman, who can be contacted via email infogov@nhs.net

15 Personal Data breaches

It is a legal obligation under Data Protection Legislation to notify Personal Data breaches within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. There is a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms. It is also a contractual requirement of the standard NHS contract to notify incidents in accordance with this guidance. By notification, this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours.

The Trusts documents all data breaches even if they do not need to be reported to the Information Commissioner.

All staff must follow the Trust's Data Security and Protection Incident Reporting Standard Operating Procedure (SOP) when an incident involving personal identifiable information has been detected. The procedure document encompasses national guidance found within the 'Guide to the Notification of Data Security and Protection Incidents' which applies to all organisations operating in the health and social care sector https://www.dsptoolkit.nhs.uk/Help/29

16 International Data Transfers

The rules around International Data Transfers only apply to UK-based businesses or organisations subject to UK Data Protection Legislation and Personal Data is being transferred to or from other countries (including European countries).

This section only applies if the Trust transfers personal data outside the UK or receives Personal Data from outside the UK. If these types of Data Flows are identifying from the annual data mapping exercise then the following guidance from the Information Commissioner on International Data Transfers will be followed.

https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/

17 Data Security Awareness Training

The Trust provides appropriate training and awareness programmes to ensure staff are aware of their responsibilities for Data Protection, Confidentiality and Information Security via NHS Digital's mandated training requirements.

All employees that have access to Personal Data undertake Data Security and Awareness training on an annual basis.

In addition to this, specialist training is compulsory for staff in specialist roles, such as the Caldicott Guardian, Senior Information Risk Owner (SIRO), Data Protection Officer, and those individuals working in specialist Cyber Security roles.

18 Monitoring & Compliance

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good security and that personal information is handled correctly

1	Following local and national policies and guidelines, what key elements require monitoring?	List elements to be monitored	a. % of staff successfully completing Data Security Awareness Training b. Compliance with all mandatory requirements within the Data Security and Protection Toolkit c. No of level 1 and level 2 data breaches reported
2	Who will lead/be accountable for monitoring?	Lead title and/or MDT	a. % of staff successfully completing Data Security Awareness Training (Data Protection Officer) b. Compliance with all mandatory requirements within the Data Security and Protection Toolkit (Data Protection Officer) c. No of level 1 and level 2 data breaches reported (Data Protection Officer)
3	Describe how the key elements will be monitored?	List tools to evidence compliance	a. successfully completing Data Security Awareness Training (Training System) b. Compliance with all mandatory requirements within the Data Security and Protection Toolkit (Data Protection Officer) No of level 1 and level 2 data breaches reported (Data Protection Officer, Informatics

			Group) c. No of level 1 and level 2 data breaches reported (Data Protection Officer via the DATIX incident reporting system)
4	How frequently will each element be monitored?	List frequency of monitoring for each element	a. successfully completing Data Security Awareness Training (monthly) b. Compliance with all mandatory requirements within the Data Security and Protection Toolkit (continuous monitoring – annual submission) No of level 1 and level 2 data breaches reported (Data Protection Officer, Informatics Group) No of level 1 and level 2 data breaches reported (Monthly)
5	Explain the protocols for escalation in the event of problems?	List the processes of escalation	a. Informatics Group b. Trust Leadership
6	Which Committee/ Panel/ Group will reports go to?	List the Committee/Panel/ Group/Peer Review that the reports will go to	a. Informatics Group
7	Explain how the policy/guideline will be disseminated within the Trust?	List ways identifying how this document will be shared and how it will be recorded that appropriate staff have been made aware of the document and where to find it	a. Notification of a new/revised policy and copies of it shall be made available to personnel via the Trust Intranet (http://wghintra01/imt/security.htm) and communicated through e-update

19 Related Policies

- Information Security Policy
- Information Governance Management Framework
- Information Sharing Policy
- ICT Acceptable Use Policy
- Data Privacy Impact Assessment (DPIA) Policy
- Data Security and Protection Incident Reporting Standard Operating Procedure (SOP)
- Incident and Serious Incident Policy

20 References

Crown Commercial Service – Action PPN 02/18
https://www.gov.uk/government/publications/procurement-policy-note-0218-changes-to-data-protection-legislation-general-data-protection-regulation.
Data Protection & Security Toolkit
https://www.dsptoolkit.nhs.uk/

UK Government (April 2020). Cyber Essential. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview. Last accessed May 2020.

21 Equality Impact Statement (EIA)

What is an equality impact assessment?

There are many benefits in conducting an equality impact assessment (EIA) prior to making business decisions about policies, clinical guidelines or any other work that may potentially impact on a wide range of people with protected characteristics. Equality impact assessments should not be seen as an afterthought once decisions have already been made.

Benefits:

- Improved capacity to consider equality, diversity and inclusion as part of business management
- Reduced costs as a result of not having to revisit a policy/project
- Take into account a diverse range of views and needs
- Enhanced reputation as a Trust that is seen to understand and respond positively and proactively to diversity.

Whatever approach you take to an equality impact assessment, case law has established that you should keep an accurate, dated, written record of the steps you have taken to analyse the impact on equality. This will help you to check whether you are complying with the duty and it will be useful if your decisions are challenged.

When completing an equality impact assessment you should consider:

- Treating a person worse than someone else because of a protected characteristic (known as direct discrimination)
- Putting in place a rule or way of doing things that has a worse impact on someone with a protected characteristic than someone without one, when this cannot be objectively justified (known as indirect discrimination)
- Treating a disabled person unfavourably because of something connected with their disability when this cannot be justified (known as discrimination arising from disability)
- Failing to make reasonable adjustments for disabled people.

Equality impact assessment process

Stage 1 (Screening)

This stage provides an opportunity to explore whether the policy decision may have a negative, neutral or positive impact on different groups of people.

- If yes, use the ‘comments’ column to describe what this impact could be.

- If no, outline how have you arrived at this conclusion.

- If unsure use the ‘comments’ column to describe what you need to do to find out.

Stage 2 (Full Assessment)
This should be carried out in compliance with policy HR028 Equality & Human Rights Policy.

Does this policy/guideline affect one group less or more favourably than another on the basis of:			
			Comments
1	Age (younger people & children& older people)	no	
2	Gender (men & women)	no	
3	Race (include gypsies and travellers)	no	
4	Disability (LD, hearing/visual impairment, physical disability, mental illness)	no	
5	Religion/Belief	no	
6	Sexual Orientation (Gay, Lesbian, Bisexual)	no	
7	Gender Re-assignment	no	
8	Marriage & Civil Partnership	no	
9	Pregnancy & Maternity	no	
	Is there any evidence that some groups maybe affected differently?	no	
	Could this document have an impact on other groups not covered by a protected characteristic? (e.g.: low wage earners or carers)	no	
	If '**NO IMPACT'** is identified for any of the above protected characteristics then no further action is required.		
	If '**YES IMPACT**' is identified a full impact assessment should be carried out in compliance with HR028 Equality & Human Rights Policy and linked to this document		

Any other comments:
Please use this box to add any additional comments relevant to the assessment

Assessment completed by:	*Nicola Bateman – Data Protection Officer*	Date completed:	26th Jan 2021

If you have any queries or concerns about completing the EIA form, contact the Trust's Inclusion & Diversity Team at WestHerts.Inclusion@nhs.net