

## Subject Access Request (SAR) Policy

<b>Department / Service:</b>	Digital Division
<b>Author/Owner:</b>	Matthew Thurland, Health Records Manager
<b>Accountable Director:</b>	Vikki Lewis, Chief Digital Information Officer
<b>Approved by:</b>	Information Governance Steering Group April 2022 Trust Management Executive
<b>Date of Approval:</b>	18 <sup>th</sup> January 2023
<b>Review Date:</b> <b>This is the most current document and should be used until a revised version is in place</b>	18 <sup>th</sup> January 2026
<b>Target Organisation(s)</b>	Worcestershire Acute Hospitals NHS Trust
<b>Target Departments</b>	All
<b>Target staff categories</b>	All

### Policy Overview:

This policy sets out the processes that are in place to manage Subject Access Requests under the UK General Data Protection Regulation (GDPR); the Data Protection Act 2018 (DPA) and the Access to Health Records Act (1990)

### Latest Amendments to this policy:

Revised in line with UK General Data Protection Regulation (GDPR)  
Revised in line with DPA 2018, Part 1, Sections 36-38 re: ATHR 1990  
Revised in line with GDPR, effective from 25.05.2018  
Revised forms for GDPR and ATHR applications

### Key Amendments made to Document

Date	Amendment	By:
December 2022	Updated to include additional guidance and minor amendments to application forms	Health Records Manager Human Resources Manager
March 2022	Updated to reflect UK GDPR and further guidance added	Health Records Manager
March 2021	Updated to include guidance on third party disclosures	Health Records Manager

## Trust Policy

November 2020	Document updated to reflect changes in Trust structure	Health Records Manager
May 2020	Document extended for 6 months during COVID period	
April 2018	Updated to reflect implementation of GDPR	Head of Legal Services
May 2017	Title change of Patient Services to Complaints, PALS and Bereavement Services	Head of Legal Services
May 2015	Updated into the most recent Trust Policy format Updated SAR health Records Guidance and Application included Reporting structure and other minor amendments included	IG Manager
Feb 2013	Policy created	IG Manager

## Contents page:

1. Introduction
  - 1.1 UK General Data Protection Regulations (GDPR)
  - 1.2 Access to Health Records Act 1990 – deceased patients
2. Scope of this document
3. Definitions
4. Principles
5. Responsibility and Duties
6. Who can make a Subject Access Request
7. Subject Access Procedures
8. Proof of Identity Requirements
9. Health Records Requests
10. Human Resources Requests
  - 10.1 Requests for email records sent from a third party where the subject is identifiable
11. Requests for electronic documents where the subject is identifiable
12. Occupational Health Records
13. Access to Leavers' Files
14. Consent Requirements
  - 14.1 Third Party Requests;
  - 14.2 Subject Access Requests made on behalf of people who lack capacity;
  - 14.3 Children and Young People
  - 14.4 Where the patient is deceased
15. Disclosure Exemptions under GDPR/Data Protection Act 2018
16. Police Requests
17. Court Orders
18. Other Requests

- 19. Medical Act 1983
- 20. Timescales for the disclosure of records
- 21. Charges
- 22. Request to view records on site
- 23. Provision of the information requested:
  - 23.1 Requests for large amounts of personal data
  - 23.2 The duty to search
  - 23.3 Manifestly unfounded or excessive requests
- 24. Third party disclosure
- 25. Redaction
- 26. Rectification
  - 26.1 When should personal data be rectified?
  - 26.2 Timescale to comply with a request for rectification
- 27. Escalation
- 28. Subject Access Requests Process
- 29. Implementation
  - 29.1 Plan for implementation
  - 29.2 Dissemination
  - 28.3 Training and awareness
- 30. Monitoring and compliance
- 31. Policy review
- 32. References
- 33. Background
  - 32.1 Financial Risk Assessment
  - 32.2 Equality Impact Assessment Tool
- 34. Consultation Process
- 35. Approval Process

### 36. Version Control

#### Appendices

Appendix 1: Subject Access Requests Flowchart

Appendix 2: Template Subject Access Request Form Employee Records (GDPR)

Appendix 3: Template Subject Access Request Form Health Records (GDPR)

Appendix 4: Template Access to Health Records Form – Deceased patients

#### Supporting Documents

1. Financial Risk Assessment
2. Equality Impact Assessment Tool

## 1. Introduction

A Subject Access Request is a request from a person asking an organisation to provide them with information relating to that person which is held or processed by the organisation.

The disclosure request may be direct (e.g. individual request for a copy of their health records) or may form part of an investigation (e.g. a request for a statement by the Police). The request may be imprecise and may be relevant to a claim against the organisation.

The person requesting the data does not need to provide a reason for requesting access however they only have a right to see information about the data subject; they have no right to see information which is not personal data or is only about third parties.

This policy provides details of the background and procedures to be followed when processing requests for access and the corresponding legislation.

### 1.1 UK General Data Protection Regulations (GDPR) & Data Protection Act 2018

The UK GDPR states that individuals have a right to obtain a record in permanent form; confirmation as to whether or not personal data concerning them is being processed and where that is the case to have access to that personal data.

The individual can access the data held about them by making a request in writing for a copy of the information the Trust holds about them, both in electronic format and in paper.

### 1.2 Access to Health Records Act 1990 (ATHR)

This Act has been repealed to the extent that it only relates to the health records of deceased patients. It applies only to records created since 1 November 1991. Applications for disclosure of records for deceased patients should only be granted to the personal representative of the estate or to someone pursuing a claim arising out of the death.

## 2. Scope of this document

This policy deals with the rights of data subjects whereby individuals can request access to their personal data.

This policy applies to all requests for access to personal data held by the Trust. This applies to anyone about whom the Trust holds information.

This policy provides a framework for the Trust to ensure compliance with the UK GDPR, DPA 2018 and Access to Health Records Act 1990. This policy is supported by operational procedures and activities as detailed in appendices 1-3.

## 3. Definitions

<b>Data</b>	The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudo-anonymized – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
<b>Personal Identifiable Information (PII)</b>	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
<b>Sensitive Personal data</b>	The GDPR refers to sensitive personal data as “special categories of personal data”. The special categories specifically include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data where processed to uniquely identify an individual, data concerning health or data covering and individual's sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
<b>Identifiable Natural Person (INP)</b>	The person the information is about and who can be identified from that information. All Identifiable Natural Persons have certain legal rights in relation to their personal identifiable information.
<b>Health Record</b>	A ‘health record’ is defined as being any record which consists of information relating to the physical or mental condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. The definition can also apply to Radiology material and if a subject access request is made, the information contained in such material must be supplied to the applicant.
<b>Employment Record</b>	An ‘employment record’ is defined as being any record which consists of information relating to a current or former member of staff and has been made by or on behalf of the Trust in connection with the individual's employment.
<b>Occupational Health Record</b>	An ‘occupational health record’ is defined as being any record which consists of information relating to the physical or mental or condition of a current or former member of staff and has been made in connection with the individual's employment.
<b>Complaint File</b>	A ‘complaint file’ is defined as being any record which consists of information relating to a complaint made by a patient or a representative acting on their behalf.
<b>Incident File</b>	An ‘incident file’ is defined as being any record which consists of information relating to an incident involving a patient; employee; contractor or visitor.

## 4. Principles

Accurately recorded information provides a platform for delivering high quality healthcare.

The Trust is committed to supporting this by:

- Providing support to patients, employees and other requesters through guidance and awareness;
- To meet legal requirements, including requests from patients or their representatives under the provisions set out in legislation;
- Promote transparency and openness;
- Provide assurance to regulatory bodies.

## 5. Responsibility and Duties

The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information, making sure it is used properly and enabling appropriate information-sharing.

The Data Protection Officer is responsible for providing advice and guidance about GDPR.

The Health Records Manager has responsibility for ensuring all Subject Access Requests regarding health records are actioned appropriately.

The Patient Safety and Risk Manager has responsibility for ensuring all Subject Access Requests regarding complaints and patient safety incidents and alerts are actioned appropriately.

The Deputy Director of People and Culture is responsible for requests by employees or former employees for copies of their personal employment files (this includes both medical and non-medical staff).

The Occupational Health & Wellbeing Manager is responsible for requests by employees or former employees for copies of their occupational health records (this includes both medical and non-medical staff)

The Chief Technology Officer is responsible for supporting SAR requests where technical searches are required in relation to the Trust network drives and NHS mail.

All staff are responsible for the efficient management and acceptable use of patient and employee records. All employees have a legal responsibility to ensure the confidentiality, integrity and availability of information is managed appropriately.

All managers must ensure their staff are aware of this policy and procedure and know how to deal with requests for personal/patient identifiable information.



## 6. Who can make a Subject Access Request?

- The data subject (such as the patient or employee)
- A person lawfully acting on their behalf:
  - Their legal representative with consent form;
  - Person with parental responsibility for under 13s;
  - Where the patient is incapable of managing their own affairs, a person appointed by the court to manage those affairs or a person upon whom the patient, when capable, has endowed an Enduring Power of Attorney or a Lasting Power of Attorney (LPA).
- Where the patient is deceased, the patient's representative (see section 12.4 below).

In certain circumstances, access may also be requested from the following bodies:

- Criminal Injuries Compensation Authority (CICA) or Department for Work and Pensions (DWP);
- The Police or Courts;
- Professional bodies e.g. Nursing & Midwifery Council (NMC), General Medical Council (GMC), Health Care Professionals Council (HCPC);
- Counter Fraud Specialists;
- Local Authority Designated Officer (LADO)

## 7. Subject Access Procedures

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them.

However, under GDPR subject access an individual is also entitled to be:

- Advised whether any personal data is being processed;
- Provided with a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Provided with a copy of the personal data on request;
- Provided with details of the source of the data (where this is available).

An individual has the right to make a request verbally or in writing and this can be made within any department in the Trust. The requestor does not need to mention the Data Protection Act or GDPR or even state that they are making a subject access request for their request to be valid, as long as it is clear that the individual is asking for their own personal data.

Requests should be referred to the relevant team for processing (outlined at Appendix 1) and a record of the request made in the log held within the relevant department.

## 8. Proof of identity

The Trust requires proof of identity before it is able to process a request. This is to protect the identity of the data subject and ensure that the Data Protection principles are upheld. Photocopies are acceptable and original documents should not be sent.

## 9. Health Records requests

All requests must contain sufficient information to enable the identification and location of the information being requested, which should be provided on the relevant application form (Appendix 3 & 4).

When requesting the records of deceased patients, a copy of the authority confirming that the requester is a personal representative of the deceased is required (where applicable this will need to be provided alongside identification).

In the case of a third party request, the Trust will verify whether they meet the legal criteria to make a request and whether they have supplied evidence to that effect (for example, written consent from the individual where this is appropriate).

The one-month timeline will begin from the date that the application form detailing the information required and proof of identity are received by the Trust.

On completion of the request, the records must be sent securely by Special Delivery to a named person or via a verified secure email system, such as NHS mail/Egress.

Documents must not be sent to personal email addresses that have not been verified as secure and advice should be sought.

## 10. Human Resources requests

Individuals can request access to their employee records. Sufficient detail to clearly identify the individual is essential and should include the person's full name, current address and payroll details such as employee number or National Insurance Number.

Where documentation provides information about third parties as well as the individual making the request, it should not be disclosed without that third party's consent, unless it is reasonable to do so.

Copies of records can be provided or alternatively personal files can be viewed on site either in the presence of the relevant manager or a member of Human Resources staff.

There is no exemption for potentially embarrassing information to be redacted or for the removal of personal comments from records. It is a criminal offence to alter, block or destroy information after receipt of a Subject Access Request.

A clear record of documents disclosed including copies of any redacted documents must be made.

### **10.1 Requests for email records sent from a third party where the subject is identifiable**

Requests can be made from current or previous staff members for the contents of email records from third parties where the subject is identifiable. This process requires authorisation from the Chief Executive Officer or Director of People & Culture to enable a search to be undertaken from NHS mail. Following this authorisation, the requests to NHS mail are made and administered by the IT Department.

NHS mail provide a full copy of the mailboxes requested. It is then the responsibility of the Trust to perform the searches in relation to the specific subject access request. After the information has been obtained, a designated Human Resources Manager will perform searches through all mailboxes for emails where the subject is identifiable. If emails are found where the subject is identifiable, third parties included in the communication are contacted to seek consent of disclosure.

### **11. Requests for electronic documents where the subject is identifiable**

Requests can also be made for electronic documents where the subject is identifiable. Where such requests are made, submissions are made via the NGSD helpdesk by a Human Resources Manager and authorisation to proceed is obtained from the Trust's third party IT service provider via the IT Department. The IT Department is responsible for making a copy of files found which are saved in a secure file path that only the designated Human Resources Manager and IT Manager can access. It is then the responsibility of the Human Resources Manager to review files for disclosure, seeking consent for disclosure and /or redaction where appropriate.

## 12. Occupational Health Record requests

Occupational Health reports or letters are held on the employee's personal file and can be disclosed with a request for the employee personal file. An employee wishing to view their full Occupational Health medical records which are held on an internal Occupational Health database will need to supply sufficient detail to clearly identify the employee and should include the person's full name, date of birth, current address and proof of identity as outlined in Appendix 2.

## 13. Leavers' files requests

Leavers' personal files should be maintained for at least six years after the employee leaves the employment of the Trust, or until the date on which the employee would reach the age of 70, whichever is the latter. Former employees may request access to their personal file.

## 14. Consent Requirements

### a. Third Party Requests

In most cases consent to access personal information will be provided by the individual who is requesting the information. However, there may be cases where the individual is unable to consent, or the individual is a child.

When a requestor is not able to produce written consent from the data subject to access their information or is not able to evidence that they are entitled to access the requested information, the Trust will require further information from the requestor, before deciding whether it would be justifiable to release the information.

In the event that the requestor is a solicitor, the subject's written authority for release must be obtained.

### b. Subject access requests made on behalf of people who lack capacity

If an adult lacks capacity and a representative is making the request on their behalf, the person processing the request must ensure that the requestor is authorised to act on the patient's behalf, that is, hold a Lasting Power of Attorney (LPA) for Health and Welfare purposes sealed by the Court of Protection.

### c. Children and Young People

A person with parental responsibility can make subject access requests on behalf of their children who are too young to make their own request.

A young person aged 12 or above is generally considered mature enough to understand what a subject access request is. They can make their own request and would need to

provide their consent to allow their parents to make the request for them. The health professional must use their own judgement to decide whether a young person aged 12 or above is mature enough to make their own request as they do not always have the maturity to do so.

Not all parents have parental responsibility. Both parents have parental responsibility if they were married at the time of the child's conception, or birth, or at some time after the child's birth. Neither parent loses parental responsibility if they divorce. However, there are circumstances in which a father who is not married to the child's mother may acquire parental responsibility for him/her.

Where a child is "looked after" by the Local Authority, permission needs to be given by both the Local Authority and the parents as they share parental responsibility.

### **d. Where the patient is deceased**

Where the patient has died, the patient's personal representative, e.g. Executor, Next of Kin (as registered on the Trust's PAS) or other authorised person may make an application for access to the relevant part of the deceased patient's health record (Access to Records Act 1990).

An application may also be made by 'any person who may have a claim arising out of a patient's death'. The decision as to whether a legitimate claim lies with the Trust and will therefore be assessed on a case by case basis, with legal advice sought as required.

In these circumstances, documents will only be provided if there is evidence that the requester was the patient's next of kin or if a will, death certificate or letter of administration can be provided.

However, this is not a general right of access. It is a restricted right and the following circumstances could limit the applicant's access:

- If there is evidence that the deceased did not wish for any or part of their information to be disclosed;
- If disclosure of the information would cause serious harm to the physical or mental health of any person;
- If disclosure would identify a third party (i.e. not the patient or a healthcare professional who has provided treatment) who has not consented to that disclosure.

The same rules apply to third party information as with other records. The Trust should afford the same level of confidentiality to a deceased person's records as for living ones.

## **15. Disclosure Exemptions under UK GDPR/Data Protection Act 2018**

The GDPR/DPA 2018 recognizes there may be valid reasons for not disclosing personal data; these are referred to as exemptions. In these circumstances, the disclosure of

information may not be viewed as SAR providing the exemption was valid. Therefore, this type of request must be considered on a case by case basis ensuring only the relevant information is disclosed to satisfy the exemption requirements.

## 16. Police Requests

The listed GDPR provisions do not apply to personal data processed for any of the following reasons:

- The prevention and detection of crime or apprehension or prosecution of offenders;
- The assessment or collection of tax or duty.

The DPA 2018 allows (but does not require) personal data to be disclosed to assist in the prevention or detection of a crime and the apprehension or prosecution of offenders.

In the first instance, the individual should be asked for their informed, explicit and signed consent to disclose the information, unless this would prejudice the enquiry or court case.

If the Police request access to either the alleged victim's or alleged perpetrator's records, consideration must be given to informing them of the request to release information so they understand the possible consequences of a future court case where this information may be shared.

Otherwise, any request by the Police to access to information held about an individual must be accompanied by the relevant Police consent form (DP2), signed by an officer at the rank of Inspector or above.

The Crime and Disorder Act 1998 also allows (but does not require) the Trust to disclose information to the Police for the purposes of preventing crime and disorder. For the Trust to consider releasing any information without consent, the access request must relate to a serious crime (e.g. murder or rape) otherwise the Police should be asked to obtain a Court Order or written signed consent.

All requests from the Police must be in writing to comply with the UK General Data Protection Regulation/Data Protection Act 2018.

## 17. Court Orders

A Court may order disclosure information. A Court Order should be obeyed unless there is robust justification to challenge it, in which case the Trust must challenge the order through the Court.

## 18. Other Requests

The same exemption can be applied to other organisations that have crime prevention or a law enforcement function. For example, Department of Work and Pensions Benefit

Fraud Section or NHS Fraud Department (NHS Act 2006).

## 19. Medical Act 1983

The Medical Act 1983 sets out the basic legislative framework for the governance of the General Medical Council (GMC). The Medical Act gives the GMC powers and responsibilities for taking action when questions arise about fitness to practice. As part of fitness to practice investigation, the GMC may request access to medical records. The registered holder must comply with this request to process and provide copies of the information held.

## 20. Timescales for the disclosure of records

It is important that action is taken promptly to process Subject Access Requests as the legislation dictates that the information must be provided without delay and at the latest within one month of receipt of the request.

The timescale for the period of compliance may be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request and an explanation given as to why the extension is necessary.

## 21. Charges

A copy of the information must be provided free of charge. However, when a request is manifestly unfounded or excessive, particularly if it is repetitive a 'reasonable fee' can be charged.

A reasonable fee can be charged to comply with requests for further copies of the same information. This does not mean a charge can be applied to subsequent access requests.

The fee must be based on the administrative cost of providing the information.

## 22. Request to view Health Records on site

It is possible for a requester to view their records on-site. In these circumstances an appointment will need to be made in advance.

Access to a record must be fully documented on the appropriate consent for release form where the visit will be supervised by appropriate staff.

In these circumstances staff must not comment or advise on the content of the record. If the applicant raises queries, then an appointment should be offered with the appropriate health professional.

The accessed record must not be removed under any circumstances and any requests for copies should be processed as a formal Subject Access request.



## 23. Provision of the Information Requested

### 23.1 Requests for large amounts of personal data

Where a large quantity of information is processed about an individual, the GDPR permits the Trust to ask the individual to specify the information the request relates to.

The GDPR does not include an exemption for requests that relate to large amounts of data, but the Trust may be able to consider whether the request is manifestly unfounded or excessive (see 22.3 below).

### 23.2 The Duty to Search

Searches need to be reasonable and proportionate. Disproportionate effort is not restricted to supply of copies but includes difficulties which occur in the process of complying with the request which may result in supply. The threshold of proportionality is high. The person dealing with the request must be able to provide evidence to show what has been done to identify personal data and the relevant plan of action. Deleted data may need to be provided depending on how difficult it is to recover.

### 23.3 Manifestly unfounded or excessive requests

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Trust can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond.

Where the decision is made to refuse to respond to a request, an explanation of the reason must be given to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. The individual should be informed of the decision without undue delay and at the latest within one month of receipt of the request.

## 24. Third party disclosure

Where records contain information that relates to an identifiable third party, that information may not be released unless:

- The third party is a health professional who has compiled or contributed to a health record, or who has been involved in the care of that individual.
- The third party gives their written consent to the disclosure of that information.
- It is reasonable to dispense with the third party's consent (taking into account the duty of confidentiality owed to that individual, any steps taken to seek his/her consent, whether he/she is capable of giving consent and whether consent has been expressly refused).



## 25. Redaction

Should the Data Controller decide that disclosure would be harmful to the data subject or any other person, the reasons for this must be clearly documented.

The reason why full disclosure has not occurred must also be communicated to the data subject. There may be some circumstances where it is appropriate for a clinical risk assessment to be undertaken and recorded within the access request process and in the clinical records.

The Data Controller must record the reasons for a decision to restrict (whether wholly or partly) the rights of the data subject and make the record available to the ICO if requested to do so.

The service will inform the data subject that their rights have been restricted; of the reasons for the restriction; of their right to make a request to or lodge a complaint with the ICO; their right to apply to a court.

## 26. Rectification

The GDPR requires that personal data shall be “accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”.

### 26.1 When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

However, diagnosis and clinical opinion are often a matter of clinical judgement. If the Trust is asked to correct data, it will take reasonable steps to investigate whether the data is accurate, and should demonstrate it has done so by considering any evidence provided.

If the personal data in question has been disclosed to others, each recipient must be contacted and informed of the rectification - unless this proves impossible or involves disproportionate effort. If asked, the individual must be informed about these recipients.

### 26.2 Timescale to comply with a request for rectification

A response to a request for rectification must be complied with within one month of receipt of the request. This can be extended by two months where the request for rectification is complex.

If a decision is taken not to take action in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the Information Commissioner.

## 27. Escalation

All queries on the operation of this policy should be referred to the Trust's Data Protection Officer.

## 28. Subject Access Requests Process

Appendix 1: Subject Access Requests Flowchart

Appendix 2: Template Subject Access Request Form Employee Records (GDPR)

Appendix 3: Template Subject Access Request Form Health Records (GDPR)

Appendix 4: Template Access to Health Records Form – deceased patients

## 29. Implementation

### a. Plan for implementation

The Data Protection Officer will raise awareness of the policy at relevant training sessions and meetings.

The Health Records Manager, Patient Safety and Risk Manager and Deputy Director of People & Culture will ensure that requests for access to records for which they are responsible are logged and processed to meet the required timescales for completion.

Staff involved with requests must be trained and be aware of the process to ensure they respond to meet the requirements and timescales detailed in the policy.

### b. Dissemination

This policy will be published on the Trust's Intranet. It is the responsibility of line managers to ensure that members of staff are made aware of this policy. New members of staff are advised during their induction process to look at the Trusts Internet and Intranet to ensure that they read and have a good working knowledge of all relevant policies, strategies, procedures and guidelines.

### c. Training and awareness

Annual data awareness training is mandatory for all staff. Any staff responsible for handling Subject Access requests must be aware of their responsibilities in complying with the General Data and Security Principle.

## 30. Monitoring and compliance

This policy will be monitored through summary updates to the Information Governance Steering Group (IGSG) from the Health Records Manager. Where requests are not

managed within the agreed timescales and standard, the steering group will request actions and monitor the improvement.

Page/ Section of Key Docume nt	Key control	Checks to be carried out to confirm complan ce with the Policy:	How often the check will be carried out:	Responsi ble for carrying out the check:	Results of check reported to: <i>(Responsible for also ensuring actions are developed to address any areas of non- compliance)</i>	Frequency of reporting:
	<b>WHAT?</b>	<b>HOW?</b>	<b>WHEN?</b>	<b>WHO?</b>	<b>WHERE?</b>	<b>WHEN?</b>
Section 19	Requests will be monitored through reporting to IGSG	Reports to IGSG	Annually	Health Records Manager	IGSG	Annually

## 31. Policy Review

The Information Governance Steering Group will review this strategy on a regular basis. Where national policy or legislation dictates change, review will be carried out at an earlier point if appropriate.

## 32. References

References:	Code:
Information Commissioner's Office – Codes of Practice	<a href="http://www.ico.org.uk">www.ico.org.uk</a>
General Data Protection Regulation (GDPR)	<a href="http://www.legislation.gov.uk">www.legislation.gov.uk</a>
Access to Health Records Act 1990	<a href="http://www.legislation.gov.uk">www.legislation.gov.uk</a>
Freedom of Information Act 2000	<a href="http://www.legislation.gov.uk">www.legislation.gov.uk</a>
Trust Information Governance Policy	WAHT-CG-579

## 33. Background

### Financial Risk Assessment

None – financial risk assessment: Supporting Document 1

### Equality Impact Assessment

None – equality impact assessment tool: Supporting Document 2

## 34. Consultation

The Policy has been updated by the Health Records Manager and circulated to those listed in the contribution list.

## Contribution List

This key document has been circulated to the following individuals for consultation:

Designation
Chief Digital Information Officer & SIRO
Deputy Chief Digital Information Officer
Chief Technology Officer
Company Secretary / Data Protection Officer
Medico-Legal Co-ordinator
Deputy Director of People & Culture
Human Resources Manager
Information Governance Manager
Information Governance Officer
Freedom of Information/ IG Officer
Deputy Chief Medical Officer/Caldicott Guardian
Patient Safety & Risk Manager
Complaints Manager

This key document has been circulated to the chair(s) of the following committees / groups for comments:

Committee
Information Governance Steering Group

## 35. Approval Process

This strategy will be approved by the Trust Management Executive.

## 36. Version Control

This section should contain a list of key amendments made to this document each time it is reviewed

Date	Amendment	By:
December 2022	Updated to include additional guidance and minor amendments to application forms	Health Records Manager Human Resources Manager
March 2022	Updated to reflect UK GDPR and further guidance added	Health Records Manager

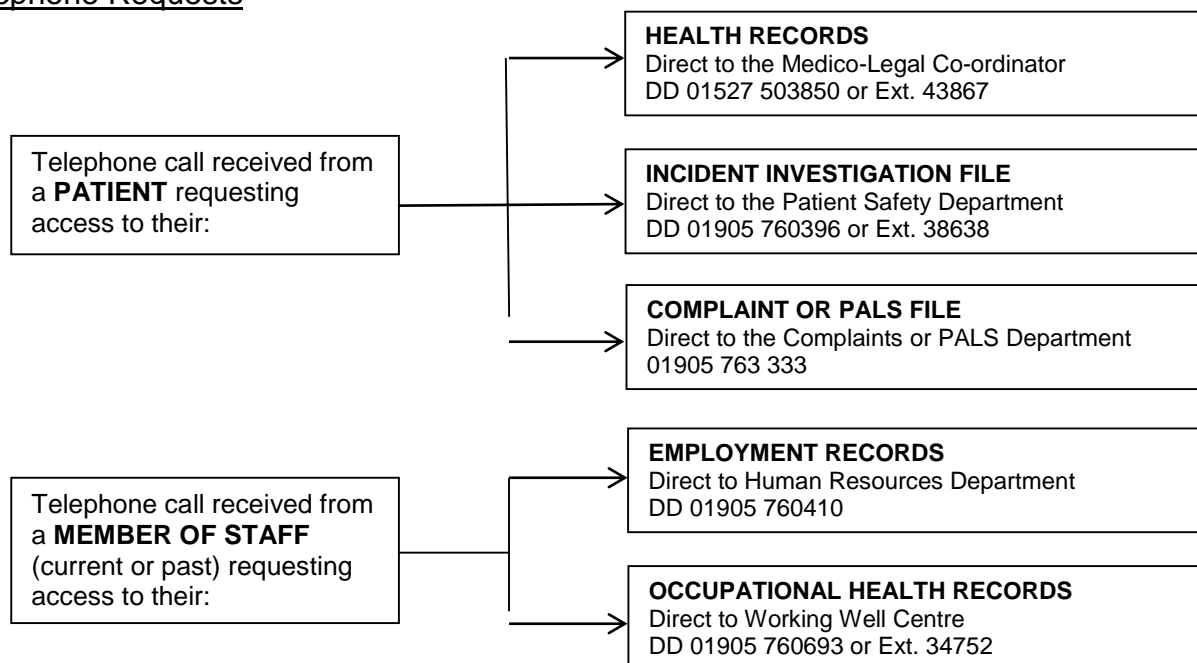
## Trust Policy

March 2021	Updated to include guidance on third party disclosures	Health Records Manager
November 2020	Document updated to reflect changes in Trust structure	Health Records Manager
July 2018	Updated to reflect implementation of DPA 2018	Head of Legal Services
April 2018	Updated to reflect implementation of GDPR	Head of Legal Services
May 2017	Title change of Patient Services to Complaints, PALS and Bereavement Services	Head of Legal Services
May 2015	Updated into the most recent Trust Policy format Updated SAR health Records Guidance and Application included Reporting structure and other minor amendments included	IG Manager
Feb 2013	Policy created	IG Manager

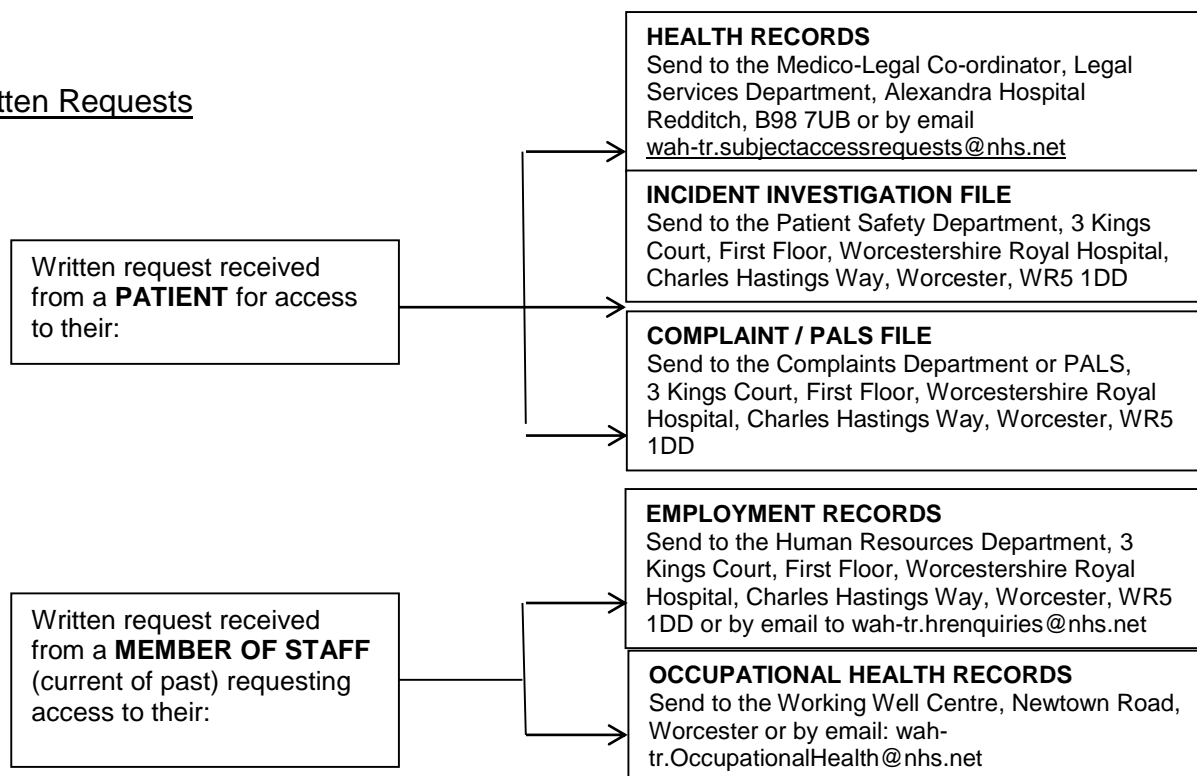
# Appendix 1 Subject Access Requests Flowchart

## Processing Subject Access Requests – if not sent directly to the correct department

### Telephone Requests



### Written Requests



All other telephone calls or written requests regarding subject access requests that do not fit within any of the categories above should be directed to the Data Protection Officer, Executive Suite, Worcestershire Royal Hospital, Charles Hastings Way, Worcester, WR5 1DD

## APPENDIX 2

### TEMPLATE FOR SUBJECT ACCESS REQUEST FORM FOR EMPLOYEE RECORDS

### ACCESS TO EMPLOYEE RECORDS UNDER THE UK GENERAL DATA PROTECTION REGULATIONS (GDPR)

#### NOTES FOR APPLICANTS

**Please read these guidance notes before completing the Application Form**

Note 1 (Part A) – Identity of the person about whom the information is requested

*This part must be completed for all applicants.*

Complete all details relating to the person whose records you wish to access. This should include former names (e.g. maiden name) and previous address, if applicable, for the period relating to the record requested.

If requesting access to health records, please refer to Appendix 3 or Appendix 4.

Note 2 (Part B) – Details of the information required.

*This part must be completed for all applicants.*

You must specify the records you wish to access and provide as many details as possible, this includes the type of document and date range of documents requested.

Note 3 (Part C) – Declaration

*This part must be completed by the person seeking access.*

Tick one box only which best describes you.

Sign and date in the space provided, and if you are not the person to who the record relates, provide your address, telephone number and relationship to the person.

You will need to supply a form of identification: either a current photo driver's licence or a current photo passport. If the person lacks capacity of understanding to make the request you also need to provide a copy of the authority enabling you to act on their behalf e.g. Lasting Power of Attorney.

We require proof of identity before we can process your request. This is to protect the identity of the data subject and ensure that the Data Protection principles are not breached. Photocopies are acceptable, DO NOT send original documents.

## Note 4 (Part D) – Authorisation for Application made on behalf of another person

This part should only be completed when the applicant is not the person to who the record relates but has been authorised by the person to make the application.

Once the details in sections A to C have been completed the person should sign and date in the space provided to officially authorise the applicant's request for access.

## GENERAL NOTES

1. WARNING – It is a criminal offence to make false or misleading statements in order to obtain information.
2. Individuals have a right to confidentiality of their personal health information and the Trust must be satisfied that an applicant is the person or the person's authorised representative. This may involve checking the identity of any of the named persons on the completed application form and their validity to request access.
3. Information may be withheld where it is considered that access might cause harm to the physical or mental health of the patient or any other individual, or where a third party might be identified.

PLEASE COMPLETE IN BLOCK CAPITALS

## APPLICATION FOR ACCESS TO EMPLOYEE RECORDS (GDPR)

### Part A – Identity of the Person about whom the information is requested (see note 1)

<b>SURNAME:</b>	<b>FORMERLY:</b>
<b>FORENAME(S):</b>	<b>DATE OF BIRTH:</b>
<b>CURRENT ADDRESS:</b>	<b>PREVIOUS ADDRESS:</b>
<b>TEL NO:</b>	<b>Email address:</b> (please provide your nhs.net email address as this is a secure domain)
<b>ASSIGNMENT NUMBER:</b>	

### Part B – Details of the information required (see note 2)

Department	Brief details of information required	Approximate Date(s)
<i>Example: Emergency Department</i>	<i>Employee personal file  Any meeting notes which identify NAME as the data subject in 2022</i>	<i>Full employee file  1/4/22 – current date</i>



	<i>Occupational Health referrals made by line manager NAME</i>	<i>Any referrals since my employment start date 1/1/22</i>

## Part C – Declaration (see note 3)

**I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the GDPR.**  
(Tick as appropriate)

<input type="checkbox"/>	I am the person named in Part A
<input type="checkbox"/>	I have been authorised to act by the person and attach their signed consent for me to access the requested data
<input type="checkbox"/>	I am the person's parent/legal guardian and have parental responsibility
<input type="checkbox"/>	The person is over 13 years of age. I am their next-of-kin/legal representative. I am making this application as they lack the capacity of understanding to make the request.

<b>SIGNED:</b>	<b>ADDRESS</b> (if different from that in Part A)
<b>PRINT NAME:</b>	
<b>DATE:</b>	
<b>TEL NO:</b>	
<b>RELATIONSHIP TO PERSON:</b>	

## Part D – Authorisation for application made on behalf of another person (see note 4)

**I hereby authorise release of my records, as specified above, to the person named in Part C and declare that I am the person named in Part A of this form.**

<b>SIGNED:</b>
<b>PRINT NAME:</b>
<b>DATE:</b>

## MUST BE COMPLETED

Please confirm the details of the identification information enclosed with the application:

	Photocopy of current photo driver's licence
	Photocopy of current passport
	Authorisation to act on behalf of a person that lacks capacity

**WARNING: It is a criminal offence to make false or misleading statements in order to obtain information.**

For employee records requests, please return the completed form along with proof of identity to:  
Human Resources Department  
3 Kings Court – First floor  
Worcestershire Royal Hospital  
Charles Hastings Way  
Worcester  
WR5 1DD or by email to: [wah-tr.hrenquiries@nhs.net](mailto:wah-tr.hrenquiries@nhs.net)

## APPENDIX 3

### TEMPLATE SUBJECT ACCESS REQUEST FORM FOR HEALTH RECORDS (GDPR)

#### ACCESS TO RECORDS UNDER THE UK GENERAL DATA PROTECTION REGULATIONS (GDPR)

#### NOTES FOR APPLICANTS

**Please read these guidance notes before completing the Application Form**

Note 1 (Part A) – Identity of the person about whom the information is requested

*This part must be completed for all applicants.*

Complete all details relating to the person whose records you wish to access. This should include former names (e.g. maiden name) and previous address, if applicable, for the period relating to the record requested. Please provide the Hospital Registration Number and NHS Number if known.

Note 2 (Part B) – Details of the information required.

*This part must be completed for all applicants.*

Please specify the records you wish to access and provide as many details as possible this includes the episode(s) of care and date range of documents requested.

Note 3 (Part C) – Declaration

*This part must be completed by the person seeking access.*

Tick one box only which best describes you.

Sign and date in the space provided, and if you are not the person to who the record relates, provide your address, telephone number and relationship to the person.

You will need to supply a form of identification: either a current photo driver's licence or a current photo passport. If the person lacks capacity of understanding to make the request you also need to provide a copy of the authority enabling you to act on their behalf e.g. Lasting Power of Attorney.

We require proof of identity before we can process your request. This is to protect the identity of the data subject and ensure that the Data Protection principles are not breached. Photocopies are acceptable, please DO NOT send original documents.

Note 4 (Part D) – Authorisation for Application made on behalf of another person

This part should only be completed when the applicant is not the person to who the record relates but has been authorised by the person to make the application.

*If the application relates to a deceased person's records, please see Appendix 4 (Access to Health Records Act 1990)*

Once the details in sections A to C have been completed the person should sign and date in the space provided to officially authorise the applicant's request for access.

## GENERAL NOTES

4. **WARNING** – It is a criminal offence to make false or misleading statements in order to obtain information.
5. Individuals have a right to confidentiality of their personal health information and the Trust must be satisfied that an applicant is the person or the person's authorised representative. This may involve checking the identity of any of the named persons on the completed application form and their validity to request access.
6. Information may be withheld where it is considered that access might cause harm to the physical or mental health of the patient or any other individual, or where a third party might be identified.

PLEASE COMPLETE IN BLOCK CAPITALS

## **APPLICATION FOR ACCESS TO RECORDS (GDPR)**

### **Part A – Identity of the Person about whom the information is requested (see note 1)**

<b>SURNAME:</b>	<b>FORMERLY:</b>
<b>FORENAME(S):</b>	<b>DATE OF BIRTH:</b>
<b>CURRENT ADDRESS:</b>	<b>PREVIOUS ADDRESS:</b>
<b>TEL NO:</b>	
<b>Email address</b>	
<b>HOSPITAL NO:</b>	<b>NHS NO:</b>

### **Part B – Details of the information required (see note 2)**

Department	Brief details of information required	Approximate Date(s)

## Part C – Declaration (see note 3)

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the GDPR. (Tick as appropriate)

<input type="checkbox"/>	I am the person named in Part A
<input type="checkbox"/>	I have been authorised to act by the person
<input type="checkbox"/>	I am the person's parent/legal guardian and have parental responsibility
<input type="checkbox"/>	The person is over 13 years of age. I am their next-of-kin/legal representative. I am making this application as they lack the capacity of understanding to make the request.

<b>SIGNED:</b>	<b>ADDRESS</b> (if different from that in Part A)
<b>PRINT NAME:</b>	
<b>DATE:</b>	
<b>TEL NO:</b>	
<b>RELATIONSHIP TO PERSON:</b>	

## Part D – Authorisation for application made on behalf of another person (see note 4)

I hereby authorise release of my records, as specified above, to the person named in Part C and declare that I am the person named in Part A of this form.

<b>SIGNED:</b>
<b>PRINT NAME:</b>
<b>DATE:</b>

Please confirm the details of the identification information enclosed with the application:

<input type="checkbox"/>	Photocopy of current photo driver's licence
<input type="checkbox"/>	Photocopy of current passport
<input type="checkbox"/>	Authorisation to act on behalf of a person that lacks capacity

**WARNING: It is a criminal offence to make false or misleading statements in order to obtain information.**

Please return the completed form along with proof of identity to:

Medico-Legal Co-ordinator  
Legal Services Department

Alexandra Hospital  
Woodrow Drive  
Redditch  
B98 7UB

or by email to: [wah-tr.subjectaccessrequests@nhs.net](mailto:wah-tr.subjectaccessrequests@nhs.net)

## APPENDIX 4

### TEMPLATE SUBJECT ACCESS REQUEST FORMS (ATHR)

#### ACCESS TO RECORDS UNDER THE ACCESS TO HEALTH RECORDS ACT (1990)

#### NOTES FOR APPLICANTS

**Please read these guidance notes before completing the Application Form**

##### Note 1 (Part A) – Identity of the person about whom the information is requested

Complete all details relating to the person whose records you wish to access. This should include former names (e.g. maiden name) and previous address, if applicable, for the period relating to the record requested.

If known, please provide the Hospital Registration Number and NHS Number.

##### Note 2 (Part B) – Details of the information required.

Please specify the records you wish to access and provide as many details as possible this includes the episode(s) of care and date range of documents requested.

##### Note 3 (Part C) – Declaration

*This part must be completed by the person seeking access.*

Sign and date in the space provided provide your address, telephone number and relationship to the person.

You will need to supply a form of identification: either a current photo driver's licence or a current photo passport, and a copy of the authority confirming you are the personal representative of the deceased.

We require proof of identity before we can process your request. This is to protect the identity of the data subject and ensure that the Data Protection principles are not breached. Photocopies are acceptable, DO NOT send original documents.

#### GENERAL NOTES

**WARNING** – It is a criminal offence to make false or misleading statements in order to obtain information.

Individuals have a right to confidentiality of their personal health information, even following their death, and the Trust must be satisfied that an applicant is the person's authorised representative.

This may involve checking the identity of any of the named persons on the completed application form and their validity to request access.

Information may be withheld where it is considered that access might cause harm to the physical or mental health of the patient or any other individual, or where a third party might be identified.

PLEASE COMPLETE IN BLOCK CAPITALS

## APPLICATION FOR ACCESS TO HEALTH RECORDS (ATHR 1990)

### Part A – Identity of the Person about whom the information is requested (see note 1)

<b>SURNAME:</b>	<b>FORMERLY:</b>
<b>FORENAME(S):</b>	<b>DATE OF BIRTH:</b>
<b>CURRENT ADDRESS:</b>	<b>PREVIOUS ADDRESS:</b>
<b>TEL NO:</b>	
<b>Email address:</b>	
<b>HOSPITAL NO:</b>	<b>NHS NO:</b>

### Part B – Details of the information required (see note 2)

Department	Brief details of information required	Approximate Date(s)

### Part C – Declaration (see note 3)

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the ATHR 1990.

<b>SIGNED:</b>	<b>ADDRESS</b> (if different from that in Part A)
<b>PRINT NAME:</b>	
<b>DATE:</b>	
<b>TEL NO:</b>	
<b>RELATIONSHIP TO PERSON:</b>	



**Please confirm the details of the identification information enclosed with the application:**

	Photocopy of current photo driver's licence
	Photocopy of current passport
	Confirmation the applicant is the personal representative of the deceased

**WARNING: It is a criminal offence to make false or misleading statements in order to obtain information.**

Please return the completed form along with proof of identity to:

Medico-Legal Co-ordinator  
Legal Services Department  
Alexandra Hospital  
Woodrow Drive  
Redditch  
B98 7UB

or by email to: [wah-tr.subjectaccessrequests@nhs.net](mailto:wah-tr.subjectaccessrequests@nhs.net)

## Supporting Document 1 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No	Comments
1.	Does the implementation of this document require any additional Capital resources	No	
2.	Does the implementation of this document require additional revenue	No	
3.	Does the implementation of this document require additional manpower	No	
4.	Does the implementation of this document release any manpower costs through a change in practice	No	
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No	
	Other comments:	No	

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval

## Supporting Document 2 - Equality Impact Assessment Tool

To be completed by the key document author and included as an appendix to key document when submitted to the appropriate committee for consideration and approval.

Please complete assessment form on next page.

# Trust Policy



## Herefordshire & Worcestershire STP - Equality Impact Assessment (EIA) Form

Please read EIA guidelines when completing this form

### Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	X	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

<b>Name of Lead for Activity</b>	Matthew Thurland, Health Records Manager
----------------------------------	--

<b>Details of individuals completing this assessment</b>	<b>Name</b>	<b>Job title</b>	<b>e-mail contact</b>
	Matthew Thurland	Health Records Manager	matthew.thurland@nhs.net
<b>Date assessment completed</b>	5 April 2022		

### Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	<b>Title:</b> Subject Access Policy			
What is the aim, purpose and/or intended outcomes of this Activity?	To provide guidance to staff on the management and processing of Subject Access Requests.			
Who will be affected by the development & implementation of this activity?	X <input type="checkbox"/> Service User	X <input type="checkbox"/> Staff		
	X <input type="checkbox"/> Patient	<input type="checkbox"/> Communities		
	<input type="checkbox"/> Carers	<input type="checkbox"/> Other _____		
	<input type="checkbox"/> Visitors	<input type="checkbox"/>		

# Trust Policy

Is this:	<input checked="" type="checkbox"/> Review of an existing activity <input type="checkbox"/> New activity <input type="checkbox"/> Planning to withdraw or reduce a service, activity or presence?
What information and evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.)	The Policy has been written in line with relevant legislation and guidance.
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)	The Policy has been widely distributed to key staff groups and the Information Governance Steering Group.
Summary of relevant findings	N/A

## Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale.** Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	Potential <u>positive</u> impact	Potential <u>neutral</u> impact	Potential <u>negative</u> impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Age		X		
Disability		X		
Gender Reassignment		X		
Marriage & Civil Partnerships		X		
Pregnancy & Maternity		X		
Race including Traveling Communities		X		
Religion & Belief		X		
Sex		X		

Equality Group	Potential <u>positive</u> impact	Potential <u>neutral</u> impact	Potential <u>negative</u> impact	Please explain your reasons for any potential positive, neutral or negative impact identified
<b>Sexual Orientation</b>		X		
<b>Other Vulnerable and Disadvantaged Groups</b> (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		X		
<b>Health Inequalities</b> (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		X		

## Section 4

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
<b>How will you monitor these actions?</b>	N/A			
<b>When will you review this EIA?</b> (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)				

## **Section 5** - Please read and agree to the following Equality Statement

### **1. Equality Statement**

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.

1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

<b>Signature of person completing EIA</b>	M. Thurland
<b>Date signed</b>	05/04/2022
<b>Comments:</b>	
<b>Signature of person the Leader Person for this activity</b>	M. Thurland
<b>Date signed</b>	05/04/2022
<b>Comments:</b>	