Status **Active** PolicyStat ID **12611612**

Origination	08/2021	Owner	Sana Sabat: Information Governance Officer
Last Approved	09/2022		
Effective	09/2022	Area	Information Governance
Last Revised	08/2021		
Next Review	08/2025		

Subject Access Request Policy

1. Introduction

Individuals have the right under current data protection legislation subject to certain exemptions, to have access to their personal records that are held by Tower Hamlets GP Care Group. This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individuals who Tower Hamlets GP Care Group (THGPCG) have had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc. All SAR requests received must be forwarded to the corporate services team at thgpcp.informationgovernance@nhs.net

2. Purpose

The purpose of this policy is to inform staff on, how to advise service users on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt.

This procedure sets out the processes to be followed to respond to a subject access request. This is based on the Information Commissioner's Office Subject Access Code of Practice.

THGPCG acknowledges the importance of openness with employees, patients, customers and other stakeholders and in co-operating with them for requests and applications to access to records or information containing their personal data.

3. Definition/Explanation of Terms

Personal Information

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, biometric and genetic data, and online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition. Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

Subject Access Request (SARs)

A Subject Access Request (SAR) is request made by or on behalf of an individual for the information about them, which is held by THGPCG. This request does not need to be in any particular format and does not need to mention that it is a subject access request. The Data Protection Legislation entitles all individuals to make requests for their own personal data to enable individuals to verify the lawfulness of how their information is being processed. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person).

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual. The Trust must provide all such information in a readable format within 30 days of receipt of the request

Information Formats

Information can be in many forms, including (but not limited to):

- Structured record systems – paper and electronic.
- Transmission of information –e-mail, post, and telephone; and
- All information systems purchased, developed, and managed by/or on behalf of the organisation.

4. Scope

The policy applies to THGPCG and all its employees and must be followed by all those who work for the

organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students. THGPCG has a legal obligation under current Data Protection Legislation including ensuring compliance with individual's right of access to personal information held by THGPCG, therefore breach of this policy will be regarded as serious misconduct and may result in:

- dismissal.
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures.
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

This procedure should be read in conjunction with the Records Management policy, which provides additional detail on the management of records within THGPCG.

This procedure covers applications to view personal information under the GDPR/DPA (2018), Freedom of Information Act (2000) and Access to Health Medical Records Act (1990).

5. Roles and Responsibilities

Chief Executive Officer (CEO)

The CEO is responsible for appointing an officer who is accountable for the management of SARs. The CEO has appointed the Executive Director of Clinical Strategy & Governance who works in conjunction with the Information Governance Officer to have responsibility for the management of SARs.

Executive Director of Clinical Strategy & Governance

The Executive Director of Clinical Strategy & Governance is responsible for overseeing THGPCG's handling of SARs requests. They will also provide support to the Information Governance Officer in the event of any challenging requests.

Caldicott Guardian/SIRO (Senior Information Risk Officer)

Caldicott Guardian/SIRO are responsible for overseeing and advising on disclosure of individual's information held by THGPCG.

Data Protection Officer (DPO)

The DPO is appointed by THGPCG and is responsible for advising on complex enquiries and ensuring compliance with regulations.

Information Governance Officer (IGO)

The Information Governance Officer is responsible for processing all Subject Access Requests (SARs) in line with THGPCG's policies and liaising with other departments and directorates for annual reporting purposes.

All Employees

Are expected and be made aware to recognise and action Subject Access Requests within one working day. These should be highlighted to the line manager and forwarded to the Information Governance Officer and/or forwarded to the Information Governance inbox.

Email

thgpcg.informationgovernance@nhs.net

Post

Executive Director of Clinical Strategy & Governance,
Tower Hamlets GP Care Group CIC
Island Health
145 East Ferry Road
E14 3BQ

6. Policy Procedural Requirements

How to recognise a Subject Access Request

In order for THGPCG to action a subject access request the following must be received:

- Requests can be made using the Subject Access Request form in appendix 3 to ensure that absolute clarity about the nature and legitimacy of the request exists.
- Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person's personal information, by reasonable means (See Appendix 1).
- The request must contain sufficient information to be able to locate the record or information requested.

A request does not need to be in any format and does not need to mention Subject Access Request. It may be made in writing (This may be by letter, fax, email, or even social media, such as Facebook or twitter). However, a request may be made verbally, where this occurs ensure that a record is made of the information requested, the date requested and by whom.

It is important to note that responses to SARs requests must be returned by a secure methodology, i.e., social media must **NOT** be used to return information requested. However, where the applicant is not able to make the request in writing it can be received verbally and a record of the request made on the applicants file.

All requests must be acknowledged and advised on timescales for response.

All requests must be responded to without delay and at the latest within one calendar month of receipt of the request. This time can be extended by a further 2 months where requests are complex or numerous. However, if this is the case you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the request relates to, or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a Freedom of Information (FOI) request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under Data Protection Legislation; and another for the remaining, non-personal information made under FOI Legislation. If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (EIR).

Any requests made for non-personal information must be forwarded to thgpcg.informationgovernance@nhs.net It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOI Legislation or the EIR is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOI Legislation or the EIR to the world at large, this could lead to a breach of the data protection principles.

All SARs requests received must be forwarded to the IG inbox thgpcg.informationgovernance@nhs.net

Data Protection Legislation does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Where requests are manifestly unfounded or excessive, because they are repetitive, you can:

1. Charge a reasonable fee considering the administrative costs of providing the information; or
2. Refuse to respond.

Where you refuse to respond you must explain to the individual, informing them of their right to complain to the supervisory authority without undue delay and at the latest within one month.

Assisting and advising data subjects in making a request

Where an individual is verbally making a request you should make a written record of the request, detailing the information they are requesting and from which service to enable its location and verify with the requestor that the record is correct.

Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request. Note some requestors may require additional assistance and therefore details might have to be supplied in an alternative accessible format.

A request is valid even if the individual has not sent it directly to the person who normally deals with

such requests. Therefore, it is important to ensure that you and your colleagues can recognise a SAR and deal with it in appropriately and ensure it is forwarded immediately to the IG officer within THGPCG who is responsible for dealing with the SAR's.

Obtain the requestors contact information and details on how they would like the response to the application to be returned to them. Note that responses to requests should be made in a format requested by the requestor, therefore alternative formats may be needed.

7. Requests on behalf of other individuals

A third party

A third party, e.g., solicitor may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g., power of attorney must be provided by the third party.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual who is the subject of the SAR rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

Requests on behalf of children

Even if a child is too young to understand the implications of Subject Access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian. It is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SARs for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request.

The Information Commissioners Office has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

The Caldicott Guardian or their nominated representative should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following should be considered:

Where possible, the child's level of maturity and their ability to make decisions like this.

- The nature of the personal data.
- Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child or young person.
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

Requests in respect of Crime and Taxation e.g., from the Police or HMRC

Requests for personal information may be made by the above authorities for the following purposes:

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

A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

These types of requests must be considered by a senior manager and the decision on whether to share the information or not must be documented before any action is taken. Advice can be sought from the Information Governance Team. Please see The Disclosure of Information to Police Policy for further guidance.

Court Orders

Court Orders requiring the supply of personal information about an individual must be complied with immediately. Please see The Disclosure of Information to Police Policy for further guidance.

8. Responding to Requests

An Information request log has been developed by THGPCG and should be used to record all the information requests received.

Determine whether the person's request is to be treated as a routine enquiry or as a SARs. Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party is obtained before releasing any information requested, this may be in the form of documentation as detailed at Appendix 3.

The following are likely to be treated as formal SARs request:

- Please send me a copy of my HR file or Medical Records.
- I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed.
- The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.

Ensure adequate information has been received to facilitate locating the information requested. Locate the required information from all sources and collate it ready for review by an appropriate senior manager. This review is to ensure that the information is appropriate for disclosure, i.e., to ascertain whether any exemptions apply e.g., it does not contain information about other individuals, it is likely to cause harm or distress if disclosed or information to be withheld due to on-going formal investigations. Advice may be sought from the Information Governance Team.

In the case of requests for clinical records these should be reviewed by the Caldicott Guardian or a nominated representative who shall decide to what extent data can be disclosed or whether the request is to be refused.

Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual. However, if information contained within the information requested was supplied by health professionals it may be disclosed without consent if considered appropriate.

Generally, THGPCG must provide a copy of the information free of charge. However, a 'reasonable fee' may be levied when a request is manifestly unfounded or excess, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact as soon as possible. It must be determined whether the information is likely to change between receiving the request and sending the response.

Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under Data Protection Legislation.

Check whether the information collated contains any information about any other individuals and if so, consider:

Is it possible to comply with the request without revealing information that relates to the third party? (Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party) Where it is not possible to remove third party identifiers you must consider the following:

- Has the third party consented to the disclosure?
- Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?

The following must be considered when trying to determine what reasonable circumstances are:

- duty of confidence owed to the third party,
- steps taken to try and obtain consent,
- whether the third party is capable of giving consent, and
- any previous express refusals of consent from the third party.

A record of the decision as to what third party information is to be disclosed and why should be made.

Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes,
- Negotiations with the requestor,
- Management Forecasts,
- Confidential References given by you,
- Information used in research, historical or statistical purposes; and
- Information covered by legal professional privilege.

Other exemptions are detailed at Appendix 2.

If the information requested, is held by the organisation and exemptions apply then a decision must be made as to whether you inform that applicant that the information is held but is exempt from disclosure or whether you reply stating that no relevant information is held. A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided. It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

If the information contains complex terms or codes, you must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms

9. Preparing the response

When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case, by the due date. A copy of the information should be supplied in a format agreed with the applicant for example if the request is received electronically, then the response should be returned in an electronic format. You have one calendar month to comply with the request starting from the date you receive all the information necessary to deal with the request. It is an offence under the Data Protection Legislation and individuals can complain to the Information Commissioners Office or apply to a court if you do not respond within this time limit.

Under no circumstances should original records be sent to the applicant. Please ensure that once copies have been made to ensure that the final version should be made into a PDF.

Remote access to records: - Where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

Ensure that the information to be supplied is reviewed by an appropriate senior manager and IG Officer and written authorisation and / or agreement of exemptions applied is obtained for disclosure or non-disclosure of the information.

10. Refusing a request

If an exemption applies, you can refuse to comply with a Subject Access Request (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information see the ICO website.

You can also refuse to comply with a Subject Access Request if it is:

- manifestly unfounded; or
- excessive.

You are exempt from complying with a SAR for health data to the extent that complying with the right of access would be likely to cause serious harm to the physical or mental health of any individual. This is known as the 'serious harm test' for health data.

You can only rely on this exemption to withhold health data if:

- you are a health professional; or
- within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health data is met. Even if you have done this, you still cannot rely on the exemption if it would be reasonable in all the circumstances to re-consult the appropriate health professional.

This means that if you are not a health professional, you cannot rely on this exemption and refuse to provide the health data in response to a SARs, unless you have obtained an opinion that the serious harm test for health data is met. Bear in mind that you may also need to obtain an opinion even if you do not intend to rely on this exemption.

The appropriate health professional is the health professional most recently responsible for the diagnosis, care or treatment of the individual. You can appoint a health professional with the necessary experience and expertise, if the most recent health professional no longer practices.

If you think this exemption might apply to a SARs you have received, see paragraph 2(1) of Schedule 3, Part 2 of the Data Protection Act (DPA 2018) for full details of who is considered the appropriate health professional.

However, if you are not a health professional, you may only disclose health data in specific circumstances.

Where it is decided to refuse a request, you must be very sure of your legal basis for doing this and you should ask your Data Protection Officer for advice. You should also inform your SIRO as they will need to make the final decision.

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action.
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

You must ensure that you fully document the decision and the reasoning behind it in case of further challenges.

11. Access to Corporate Information

THGPCC is subject to the provisions of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. Personal Data is usually exempted from public disclosure but in certain circumstances some personal data may be disclosed in the public interest but still subject to the individual's rights under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018.

12. Retention Schedules

Retention Schedules from the Records Management Code of Practice for Health and Social Care 2016 will be applied to all requests 3 years after the last recorded action and then will be destroyed under confidential conditions. Where the response to a request has resulted in an appeal, these requests will be kept for 6 years after the last recorded action and then will be destroyed under confidential conditions.

13. Requests Relating to Children

Where requests relate to information held about a child it is important to determine whether there is a legal right to access those records. It is important to consider the following**:**

- The duty of confidentiality owed to the child.
- Whether disclosure could result in serious harm to the individual or any other person. and
- Those children under the age of 13 who have capacity to take decisions about treatment to which they are entitled to.

14. SARs for Employees

Under GDPR/DPA (2018), employees have a right to request all the information their employer holds of them. This process is the same process as a typical SAR, and is as follows:

- The information is reviewed by an administrator nominated by the Human Resources Department who will consider any exemptions, redactions and third party information
- Identity checks and details for the request are the same as in the procedure above. However, it is accepted that if an employee is known to the organisation, this may provide sufficient proof of identity
- The employee can request to view original records but subject to the ability to resource and assist and may have pre-conditions. The judgement of the Human Resources will be sought in assisting these requests.

NOTE: Under GDPR/DPA (2018), employees are able to access any emails retained by the organisation that refers to them.

15. Power of Attorney

Anyone who holds Power of Attorney is entitled to be given access to that person's staff or medical record subject to the proper scrutiny of appropriate evidence. Appropriate evidence is sight of the original document giving Power of Attorney, a photocopy of which should be retained.

16. Deceased Persons

Under the terms of the Access to Health Medical Records Act 1990 (AHMRA), requests can be made to access the health records of a deceased person. Under the terms of the Act the following have a right to request access:

- The patient's personal representative, this is the executor or administrator of the deceased person's estate.
- Any person with a claim arising out of the patient's death.

The personal representative has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record.

Should an AHMRA be received relating to a deceased member of staff, the Director of Quality & Assurance must ensure that the person making the request is entitled to receive the information, such as Power of Attorney (see above) or as their Executor (see below).

In all circumstances, the identity of the requester and any relationship to the deceased must be proved. The serious harm and third party confidentiality rules will still apply. It may be necessary to refer more sensitive cases to the Caldicott Guardian where appropriate.

17. Redactions

Following review and consideration of the collated response to the request by the Information

Governance Team and the Caldicott Guardian, any data which is agreed to be removed would need to be redacted from the data prior to release. This is normally under the supervision of the IGO, DPO and Executive Director of Clinical Strategy & Governance.

Important: Original records must never be redacted. Only copies of the original must be redacted. if requested for disclosure with particular attention paid to reported opinions of third parties.

Redaction Entries

Data Subjects, or those acting for them, have the right to request the erasure or amendment of any entries in a personal record that they believe to be factually incorrect and the record holder must consider any such petition made by the data subject, this is by virtue of Article 16 GDPR. If, however, the record holder believes the statements in question to be accurate, and is therefore unwilling to amend them, the subject has the right to have recorded in the employee or medical record the fact of this dispute.

Any such requests should be discussed with the relevant service lead, IGO and the THGPCG Executive Director of Clinical Strategy & Governance for guidance and advice.

18. Release of Records

Once you have received the relevant information and identification, the records can be released. On no account must the original record be released.

If you are denying or restricting access, you do not have to give a reason for the decision but you should be willing to direct the subject through the appropriate complaint's channels.

Where information is not readily intelligible, an explanation (e.g., of abbreviations or terminology) must be given.

If it is agreed that the subject or their representative may directly inspect the record, a health professional or HR administrator must supervise the access

19. Dealing with Complaints

If an applicant is unhappy with the outcome of their access request, the following complaints channels should be offered:

- For employees the HR or health professional may wish to have an informal meeting in an effort to resolve the complaint locally
- If the HR or health professional feels that they cannot do anything for the data subject locally the matter should be referred to the Data Protection Officer.
- The data subject may not wish to take this route and, alternatively, may want to make a complaint direct to the Information Commissioner at:

  Information Commissioner's Office (ICO)
  Wycliffe House

Water Lane Wilmslow
Cheshire
SK9 5AF
Website: www.ico.org.uk
Telephone: 0303 123 1113
Information Line: 01625 545 745
Email: notification@ico.org.uk

20. Further Advice

Further advice may be obtained from the Information Governance Officer , Data Protection Officer or the Executive Director of Clinical Strategy & Governance.

21. Review

This policy will be reviewed every 3 years, or earlier if there are changes to National Guidance or significant changes to the management of risk across the organisation.

22. Dissemination and Implementation

Upon approval, the policy will be shared with all employees through the 'all staff' email, and also updated on THGPCG intranet page. A team and management briefing will be provided to support this dissemination

23. Appendices

Appendix 1: Registration & Authentication Examples of Documentary Evidence

Appendix 2: Subject Access Request Exemptions

Appendix 3: Subject Access Request Form

Appendix 4: Request to Access Personal Records of the Deceased

Appendix 5: Acknowledgment Letter

Appendix 1 - Registration & Authentication Examples of Documentary Evidence

Please supply one from each of the following categories (copies only).

Personal identity

- Current signed passport
- Residence permit issued by Home Office to EU Nationals on sight of own country passport
- Current UK photocard driving licence
- Current full UK driving licence (old version) – old style provisional driving licenses are not acceptable

- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the right to benefit
- Building industry sub-contractor's certificate issued by the Inland Revenue
- Recent Inland Revenue tax notification
- Current firearms certificate
- Birth certificate
- Adoption certificate
- Marriage certificate
- Divorce or annulment papers
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms);
- GV3 form issued to people who want to travel in the UK but do not have a valid travel document
- Home Office letter IS KOS EX or KOS EX2
- Police registration document
- HM Forces Identity Card Active in the Community "Active in the Community" documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the name and address of the registrant.
- Record of home visit
- Confirmation from an Electoral Register search that a person of that name lives at that address
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- Local authority tax bill (valid for current year)
- Current UK photo card driving licence (if not used for evidence of name) NY-116 – Subject Access Request Policy – November 2020
- Current full UK driving licence (old version) (if not used for evidence of name)
- Bank, building society or credit union statement or passbook containing current address
- Recent original mortgage statement from a recognised lender
- Current local council rent card or tenancy agreement
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- Court order

Active in the Community

"Active in the Community" documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the name and address of the registrant.

- Record of home visit
- Confirmation from an Electoral Register search that a person of that name lives at that address
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- Local authority tax bill (valid for current year)
- Current UK photo card driving licence (if not used for evidence of name) NY-116 – Subject Access Request Policy – November 2020
- Current full UK driving licence (old version) (if not used for evidence of name)
- Bank, building society or credit union statement or passbook containing current address
- Recent original mortgage statement from a recognised lender
- Current local council rent card or tenancy agreement
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- Court order

Appendix 2 - Subject Access Request Exemptions

This is not an exhaustive list, for comprehensive information on how to apply exemptions see the code of practice.

Category	Exemption
National Security	Personal information that is held in respect of the maintenance of national security is exempt from disclosure.
Crime and Taxation	Section of the personal information contained in the records, or individual records that relate to the prevention and detection of crime or the apprehension or prosecution of offenders.
Health, Education and Social Work	Health exemptions are mentioned in section 7 Social work records exemptions comes under the Data Protection (Subject Access Modification)(Social Work) Order 2000 relates to personal information used for social work purposes: Where release of information may prejudice the carrying out of social work by causing serious harm to the physical or mental condition of the data subject or others. Certain third party's information can be released if they are a "relevant person " (a list is contained in the order) as long as release of the information does not cause serious harm to the relevant person's physical or mental condition, or with the consent of the third party
Regulatory activity	Personal data processed by the PCT for the purposes of discharging it functions are exempt if the release of such information would prejudice the proper discharge of those functions.
Research, history	Where the personal data is used solely for research purposes and as long

statistics	as resulting statistics are not made available which identify the person
Human fertilisation and embryology	Personal information can be withheld in certain circumstances where it relates to human fertilization and embryology.
Legal Professional Privilege	Any correspondence to or from or documentation prepared for or by the Trust's internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information.

Appendix 3: Request to Access Personal Records

Please see the attached Appendix 3: Request to Access Personal Records

Appendix 4: Request to Access Personal Records of the Deceased

Please see the attached Appendix 4: Request to Access Personal Records of the Deceased

Appendix 5: Acknowledgement Letter Template

Please see the attached Appendix 5: Acknowledgement Letter Template

24. Equality Impact Assessment

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval

Policy Name: Subject Access Request
Name of Assessor: Ruth Walters

		Yes/No/ Possible/ Not Applicable	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race	No	
	Religion or belief	No	
	Disability – learning disabilities, physical disability, sensory impairment and mental health problems	Possible	Written request may not be possible. In this situation advice should be sought from the Director of Quality & Assurance as indicated on the form
	Gender	No	
	Sexual Orientation	No	
	Age	No	

2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

Attachments

- Appendix 3: Request to Access Personal Records
- Appendix 4: Request to Access Personal Records of the Deceased
- Appendix 5: Acknowledgement Letter Template

Approval Signatures

Step Description	Approver	Date