|  |  |
| --- | --- |
| **Policy/Procedure Title:** | **Subject Access Request Procedure** |

|  |  |
| --- | --- |
| **Domain** | Information Governance  |
| **Number** | IG X |
| **Main author** |  | **Ratified by** |  |
| **Date Written** |  | **Ratification date** |  |
| **Date Distributed** |  | **Review date** | Should be reviewed annually |
| **Responsible Group/person** |  | **Ratified by** |  |

|  |  |  |
| --- | --- | --- |
| **Version Number:** | **Date:** | **Supersedes Version No:** |
| V1 |  |  |

These procedures are applicable to staff employed by and/or working for and/or delivering services to or on behalf of (whether directly or through sub-contract arrangements) the following organisations:

These procedures apply to the following group(s) of staff:

|  |  |
| --- | --- |
| **Staff Group** | **Yes** |
| Head Office | ✓ |
| All staff  | ✓ |
| Volunteers | ✓ |
|  |  |
|  |  |
| Specific staff group(s) (if applicable, please state group(s) |  |

Signed on behalf of ………………………………..:

…………………………., Chief Executive Date: ………………………….

Contents

1. Subject Access Request (‘SAR’) Procedures 3
2. What is a subject access request 4
3. Glossary 4
4. Who can make a subject access request? 4
5. What is a valid SAR 5
6. Do you have enough information to be sure of the requester’s identity? 5
7. Do you need any other information to find the information they want? 5
8. What fee do I charge? 6
9. Do I need to log the request? 6
10. How to log a request on the logging spreadsheet 6
11. How long do I have to respond? 6
12. The responsible Healthcare Professional (if appropriate) 7
13. What information should be provided? 7
14. Is there anything which should not be included? 7
15. May cause serious harm 7
16. Information relating to or provided by a third party 7
17. How to redact (edit or remove) 8
18. What should I do to complete the request? 8
19. Accompanying letter 9
20. Final tasks 9
21. Safeguarding issues 9
22. Children’s information 10
23. Sending information abroad 10
24. Request from a Solicitor 10
25. Requests from other authorities 11
26. Access to information relating to deceased persons 11
27. Repeated, unreasonable requests 11
28. Amendments or deletions from information 11
29. Retention of information 11
30. Access to Medical Reports Act 1988 12
31. Criminal Injuries and Compensation Authority 12
32. Can MPs have access to information about their constituents? 12

Example letter seeking further information 13

Standard Response letter 14

Summary of requestor types and actions to take 15

Other useful information

1. Subject Access Request Procedures

Receive verbal/written request for information

Who is it from?

Is it a valid request?

Sure of requester’s identity?

Record request on logging sheet and acknowledge receipt

Pass details to responsible person

Ascertain which information is required and compile

Yes

Seek proof of identity

Request further information

Receive further information

No

Ascertain which information is required and compile

Examine data

The data reveals the identification of a third party

Yes

No

The third party consents to disclosure in writing

Send data to applicant with covering letter (electronically or recorded delivery)

No

It is reasonable to disclose without consent

Send data with third party information (electronically or recorded delivery)

Send data with third party information (electronically or recorded delivery)

Yes

Yes

Yes

No

Send data excluding third party information (electronically or recorded delivery)

Update logging sheet with date sent and number of days it took to complete request

See sections on:

Children’s information Sending information abroad

Solicitor’s requests Request from other authorities

Deceased persons Repeated, unreasonable requests

Amendments/Deletions in information Retention of information

Under the GDPR no fee may be charged *unless:*

The requests are repetitive or excessive, the request is for further copies of the same information on the same occasion

1. What is a Subject Access Request?

A Subject Access Request (‘SAR’) is a request received from a person asking to provide them with copies of the information held about them. Individuals have this right under the Data Protection Act 1998 (‘DPA’).

Right of access extends to all information held on an individual and includes paper and electronic files, photos, recordings, emails, etc. referring to the individual.

The Act stipulates that the data subject must:

Make the request in writing

Supply information to prove who they are (to eliminate risk of unauthorised disclosure)

Supply appropriate information to help the organisation to locate the information they require.

The data subject is entitled to:

Information on whether or not the personal data are processed (see glossary below)

A copy of the data in permanent form (subject to important exemptions described in this procedure).

An explanation of any codes/jargon contained within the data.

The organisation must respond to Subject Access Requests within 40 days as stated in the Data Protection Act however it is good practice to comply within 21 days.

1. Glossary

Data Information which has been gathered by the Data Processor (the organisation)

Personal Data Information relating to a living individual which identifies them

Data Subject The individual who is either the direct subject of the personal data, or can be identified from it

Processing Any actions in relation to the data such as holding, disclosing, using, erasing, destroying, etc.

Third Party A person other than the data subject eg. Solicitor, family member, etc.

GDPR General Data Protection Regulation – to come into effect on 25 May 2018

1. Who can make a Subject Access Request?

Any individual (data subject) can make a SAR for their own information.

The data subject may nominate a representative (such as a solicitor or relative) to apply on their behalf, however, the request must be authorised by the data subject.

A child may apply and a person with parental responsibility can apply for a child’s information. There are a number of considerations (see the section on Children for further explanation).

Refer to Appendix 1 for guidance on mental capacity. There are no specific legislative SAR provisions for someone who is mentally incapacitated, however, the Mental Health Act 1983, Section 130B, contains a section on Independent Mental Health Advocates accessing patient medical records which may apply. A link to this document may found in the references section of this document.

1. What is a valid SAR

All requests should be in writing unless there is a clear reason why this is not possible. We cannot insist the data subject completes a form.

If the request is from a solicitor see section ‘Request from a solicitor’

A valid SAR should be in writing unless the person is unable to provide a written request. An email or request via social media is acceptable but you must be satisfied of the person’s identity.

Sufficient information is needed about the data subject in order to locate the correct information; eg full name, address, date of birth.

A correspondence address is essential, a telephone contact number is useful but not essential.

A clear request for the information should be made although this does not need to be for everything we hold, it can be for part of the information we have.

The Act that the data subject is using to support their application does not have to be stated and no reason needs to be given. We can ask why a data subject requires the information but they do not have to tell us.

If the request is for another organisation or does not cover the information we hold let the Information Governance Lead know immediately in order for it to be returned to the sender.

1. Do you have enough information to be certain of the requester’s identity?

Often you will have no reason to doubt a person’s identity, e.g. you may know them well.

If a person with whom you have regular contact sends a letter from their known address it may be safe to assume they are who they say they are. If you have cause to doubt the requester’s identity you can ask them to provide any evidence you reasonably need to confirm it.

Examples of proof of identity are driving licence, passport, work ID badge or bus pass; proof of residence are current bank statement, pay slip, utility bill or a letter on headed paper from local authority etc. You should ask for one of each type.

An example letter requesting further information can be found at the end of this Policy.

1. Do you need any further information to find the information requested?

You must be prompt if you require the data subject to provide any further information you reasonably need to find the information requested.

You might want them to narrow down their request. For example the data subject may only be interested in information relating to a particular incident, piece of advice or care given or relating to a particular time frame.

An example letter requesting further information can be found at the end of this Policy.

1. What fee do I charge

At the moment we can charge a fee of £10 which would be appropriate for a request for a large amount of information.

From 25 May 2018 this fee will not be chargeable. We will only be able to request a fee should the data subject request more than one copy of the same information as part of one SAR; or if the requests made by one person are repetitive and unreasonable. Please ask your IG Lead for further advice if this is the case.

1. Do I need to log the request?

Yes.

The recording of requests gives us an accurate and complete audit trail. This is particularly useful if any further requests are made or we are asked to investigate an action or piece of advice.

All applications must be recorded in the data subject’s notes.

Use the attached logging spreadsheet to keep a record on the request. This also contains a tool which will work out the date for compliance for both 21 and 40 days. The working copy of this spreadsheet is ……………………………………………………

1. How to log a request on the logging spreadsheet

Always ensure you action requests immediately in line with our process. The logging spreadsheet should be used to log the request. If you are not the person processing the request it will start the process of logging and avoid any delay in meeting the required timescales.

Open the logging spreadsheet, which is saved on ………………………………… and enter the initials and day from the data subjects date of birth, eg JH23 for Jon Howard born on 23 January 1965.

Complete the remainder of the required information under the headings and save the document. Do not make separately copies of the log.

1. How long do I have to respond?

Once you have received all the information you need to help you find the requested information the Data Protection Act states that requests for access to information should be met within 40 calendar days. Best Practice and government guidance suggests all organisations should aim to respond within 21 calendar days.

The responsible person should be informed a SAR has been received in order for them to set aside the time to review the information prior to it being given to the data subject or requestor.

1. The responsible Healthcare Professional

If you provide clinical care to the Data Subject then the Data Protection Act Order 2000 instructs the most recent Healthcare Professional involved in recording information regarding the clinical care of the person to be consulted to assist with the SAR. If there is more than one Healthcare Professional then the most appropriate, available Healthcare Professional should be approached.

1. What Information should be provided

Staff need only provide the part of the record which relates to their service.

If the Data Subject (or their representative/requestor) requests information from more than one service then one person should be responsible for collating the information.

If the Data Subject (or their representative/requestor) requests all information available one person should be responsible for collating the information.

If printed copies of the information are to be sent to the Data Subject they should be reviewed prior to posting.

If the information contains incident reporting forms check for third party data.

Electronic information can be printed or sent directly once checked for third party data.

Check for requests for photography, cctv etc.

1. Is there anything which should not be included

Under the Data Protection Act there are two main reasons where access could be denied or limited to a Data Subject or their authorised representative.

* Where the information could cause serious harm to the physical or mental health or any related condition of the data subject, or any other person; or
* Where the information would disclose information relating to or provided by a third party who had not consented to that disclosure.

The responsible person should check these do not apply prior to releasing information. Be aware there is no exemption from revealing poorly framed opinions and/or personal remarks which could be open to misinterpretation and possible constitute slander or libel.

1. Serious Harm

You may believe the information may provide the Data Subject with information about their health, mental wellbeing or situation which may cause serious harm to their health, mental wellbeing or to that of another person. If so The Data Protection Act (Subject Access Modification (Health)) Order 2000 allows you to withhold the information. As the consideration is towards the Data Subject’s physical or mental health a Healthcare Professional will be required to support the decision. This decision must be fully documented in the logging sheet. The exemption does not apply to information the Data Subject already knows.

The responsible person for IG must be aware of the information and decision taken.

1. Information relating to or provided by a third party

You can disclose information exchanged between people in the organisation.

Where information has been provided by another organisation or in a multi-disciplinary setting you must contact all third parties and explain you would like to include that information.

Do not disclose any information from a third party without that person’s consent unless it is reasonable to do so.

A third party is anyone who is not the subject of the information. A third party will therefore be family members, friends, carers, a social worker, staff from the local Council, neighbour, other advisor etc.

e.g. John Smith’s service user information may contain a reference to his sister, Jane. John is entitled to see what has been recorded about him but not information relating to Jane.

Information about third parties will need to be redacted (edited out) or their consent to disclose sought.

Supply as much information as possible by editing the references to other people (see how to redact below).

Make sure any abbreviations, codes or technical terms are explained so the information can be understood.

You can make routine amendments to the record after receiving a request *but* you must not make any changes to the information as a result of receiving the request even if you find inaccurate or embarrassing information will be included.

17. How to redact (edit or remove)

To redact information which must not be revealed you can:

Take a copy of paper information, use a black marker pen or correction fluid to block out exempt data and photocopy again to give to the requested. Be aware that you should double check the re-photocopied sheets to make sure the data is not legible.

Block out an electronic copy using black highlighter but you must then print and scan the document and send the scanned copy. Do not send a ‘Word’ document as the highlighted can be ‘undone’ and do not PDF as a PDF can also be reversed.

The safest way to redact hard copy documents is to copy the original document, cut out the redacted section and re-copy the remaining text.

You should make a note of what has been redacted and why the information was removed. You may be asked to justify this in a legal situation.

18 What should I do to complete the request?

Once the disclosure has been approved according to your local procedure the copy of the information may be sent to the Data Subject or requestor in a sealed envelope by recorded delivery. It should be marked ‘Confidential for Addressee only’.

You can send information electronically if requested. You should ensure the recipient is aware that email is not secure. You should be certain the email address is that of the Data Subject or requestor. It is appropriate to send a test email first to ask the recipient to confirm you have the correct email address. You should also add a ‘read receipt’ to your email. All attachments should be password protected and the password supplied by a different media if possible, e.g. text message. If it is only possible to use the email address the password should be sent in a separate email.

Only copy information should be sent – not originals.

No confidential information should be sent by fax.

The Data Subject can collect the information however it is important to ensure you know them or have asked them to bring ID. They should sign to say they have received the information.

You have a duty under the Equality Act 2010 to assist applicants by ensuring the information is in the form most suitable for them.

You must also provide them with information on how to make a complaint.

19 Accompanying letter

You should provide a letter which includes a description of the information confirming that this is the information available to them under the Data Protection Act 1998 (to be replaced by the General Data Protection Regulation – to come into effect on 25 May 2018). You should explain why you keep the information, a list of people to whom you may routinely disclose the information and an explanation of why you may do so.

Example letters are available at the end of this procedure.

The organisation is under no obligation to disclose to the applicant whether it has withheld any of the information held. If you receive a direct request asking if you have disclosed all held information you may reply that the organisation has fully discharged all of their obligations under the Act.

20 Final Tasks

Information taken out of normal storage for this process should be returned to its main place of storage as soon as possible after completion of the request.

Electronic information should not have been affected however if part of the electronic record has been saved as a separate document, eg a ‘word’ document it should be saved securely. Do not save on the Desktop.

Update the log with your actions and the time taken.

Any information which breach 21 days should be reported as an incident to enable our organisation to respond to any training needs or identify how we can improve in the future.

21 Safeguarding Issues

If there are Safeguarding issues you should especially consider the information carefully to ensure it will not damage the Data Subject’s physical or mental wellbeing. If you are particularly concerned the Data Subject has been coerced to request information you should seek further advice. If you are in touch with your local Safeguarding Team/Social Services/named social worker for the Data Subject you can raise your concerns in the usual way. You will need to change this to reflect what you would do to raise Safeguarding concerns.

22 Children’s information

Even if a child is too young to understand the implications of subject access rights data about them is still their personal data and does not belong, for example, to a parent or guardian. So 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.

* Anyone with parental responsibility has a statutory right to apply for access to their child’s health records and other information
* Release of records/information is usually only made in the best interests of the child
* Before responding to a SAR for information held about a child you should consider whether the child is mature enough to understand their rights (Gillick competency and Fraser guidelines are available on-line or you may wish to seek legal advice as this is a complex area)
* If you are confident the child can understand their rights then you should respond to the child rather than a parent. 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 you should take into account, amongst other things:
	+ The child’s level of maturity and their ability to make decisions
	+ 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 those with parental responsibility having access to the child or young person’s information
	+ Any detriment to the child or young person if the individual with parental responsibility cannot access the information; and
	+ Any views the young person has on whether parents should have information about them
* If the child is not competent you should allow the parent to have the information as long as it is in the Child’s best interest
* Where parents are separated and one applies for any information you hold you are not obliged to inform the other parent.

It is not acceptable to assume that if a decision is made that a child or young person is competent to make a SAR that child or young person also has capacity to consent to share their information, they may not understand the implications of doing so.

23. Sending information abroad

 The procedure for sending personal information to someone in the EU is identical to that of the UK.

 If asked to send information to countries outside the UK you should consider each case individually, taking into account need to verify identity, security of data in transit, removal of any third party information.

24 Request from a Solicitor

 The procedure for requests from a Solicitor is very similar. The Solicitor may or may not be acting on behalf of the Data Subject.

* If the Solicitor is requesting information on behalf of the Data Subject you should receive/request a letter or authority from the Data Subject.
* If the Solicitor is requesting information about a deceased person the executor of the estate should grant consent to the release of the information. This may, or may not, be the Solicitor.
* If the request pertains to a potential claim against the organisation the CEO should be informed immediately

25 Requests from other authorities

 See Appendix.

26 Information regarding deceased persons

* Health Records fall under the Access to Health Records Act (1990) and relates to information dated after 1 November 1991.
* Other information can be provided but should only cover information recorded by the organisation. No third party information should be provided.
* You should consider who is requesting the information. You may wish to follow guidance similar to that covered by Health Records. The information can only be provided to a personal representative of the Data Subject or someone who has a claim resulting from their death.
* If you are not sure the Information Commissioners Office may be able to provide you with advice or you should check with a legal advisor.

27 Repeated, unreasonable requests

The Data Protection Act does not limit the number of Subject Access requests an individual can make to any organisation however it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says there is no obligation to comply with an identical or similar request to one already dealt with unless a reasonable time interval has elapsed between requests.

The Act suggests considering:

* The nature of the information requested – is it particularly sensitive
* How often data is altered – if information is unlikely to have changed then the decision not to respond to the same request twice would be supported

28 Amendments to or deletions from Information

If the Data Subject receives their information and thinks there is something wrong they should discuss it with the organisation.

29. Retention of Information

A copy of the letter which sets out the outcome of the request should be kept with the Data Subject’s information and should be retained in line with organisational retention processes.

A copy should be kept with all information relating to SARs and can be disposed of 3 years after the last action. They must be destroyed confidentially.

If an appeal is made to the ICO the information should be kept for 6 years after the outcome of the appeal.

30 Access to Medical Reports Act 1988

This may not apply to your organisation.

This Act governs access to medical reports made by a medical practitioner who is or has been responsible for a patient’s clinical care. These may be, for example, for a potential or existing employer or an insurance company. Consent should be given by the Data Subject.

31 Criminal Injuries and Compensations Authority (CICA)

 Third party requests may be received from Solicitors, The CICA etc requesting information. The Data Subject must provide consent.

32 Can MPs have access to health information about their constituents?

 The Data Protection (Processing of Sensitive Personal Data (Elected Representatives) Order 2002 enables information to be disclosed to elected representatives without contravening the Data Protection Act 1998. Normal procedures, however, should be followed and consent should be obtained from the Data Subject. The ICO website contains guidance on this or legal advice may be sought.

Example Letter 1 – Seeking further information

Reference

Date

Name and address of requestor

Dear

Access to personal data under the Data Protection Act 1998

Thank you for your application dated xxxxxxxxxxxxxx requesting information the organisation holds about you in our records.

Use paragraphs below as appropriate

As some of the information we have may be sensitive, for security reasons, we would be grateful if you would provide proof of identity and proof of residence.

Examples of acceptable proof are photo Driving Licence, Passport of work ID badge, bus pass or a witness to your signature on headed notepaper from a Doctor/Solicitor. Proof of residence would be a current bank statement, payslip, utility bill or letter from the local authority.

As a parent, foster parent or carer of a child and you are requesting information about the child, we will need evidence of your identity (see above) as well as proof of parental responsibility, e.g. full birth certificate, legal guardianship or evidence from Social Services.

As the information you are requesting is not about you we would need you to provide proof of your identity (see above), proof of the identity of the Data Subject and proof of your right to act on their behalf.

Your request for all personal data that we may hold about you is not specific and we would be grateful if you would let us know more specifically what information you are seeking. Further information would include dates or range of time, details of the person you were speaking with or any reference numbers relating to your request. This will enable us to locate the specific information you are requesting.

Once we have received your reply your request will be dealt with as quickly as possible and, in any event, within the 40 day limit set by the Act. The 40 days will start from the date on which we receive the information.

If you are unhappy with the way we have dealt with your subject access request you may write to:

Xxxxxxxxxxxxxxx

CEO or usual name and address for any complaints

Should you remain dissatisfied you may contact the Information Commissioners Office at:

<https://ico.org.uk/concerns/>

Or call them on 0303 123 1113

Yours sincerely

Xxxxxxxx

Job Title

Example Letter 2 – Standard Response Letter

Include ‘What we do with your information’ leaflet

Reference

Date

Name and address of requestor

Dear

Request for information regarding xxxxxxxxxxxxxxxxxx

Thank you for your letter of xxxxxxxxxxxx requesting information.

I enclose the information requested and confirm this is the information you are entitled to under the Data Protection Act 1998.

Where any abbreviations have been used these are explained on a separate sheet.

I have enclosed a leaflet explaining what we do with the information you provide and any record of the care or advice we have given.

If you have any questions about the information provided please do not hesitate to contact me.

If you are unhappy with the way we have dealt with your subject access request you may write to:

Xxxxxxxxxxxxxxx

CEO or usual name and address for any complaints

Should you remain dissatisfied you may contact the Information Commissioners Office at:

<https://ico.org.uk/concerns/>

Or call them on 0303 123 1113

Yours sincerely

Xxxxxxxx

Job Title

Summary of requestor types and actions to take

|  |
| --- |
| Quick Access guide to requests and required actions |
| Data Subject | ✓ | People we have seen can request access to any of the information we have recorded |
| ✓ | The person does not need to say why they want the information |
| ✓ | The request should be in writing  |
| 🗶 | Do not confirm you have any information until you are certain the person asking is the Data Subject |
| Solicitor | ✓ | Solicitors/Insurance/Medical companies acting on behalf of our service user may make an application for access to the Data Subject’s records |
| ✓ | Written consent from the Data Subject will be required |
| ✓ | If you are not certain you should contact the Data Subject to be sure they understand you are releasing information to a third party |
| Police | ✓ | Police may request information with the consent of the Data Subject |
| 🗶 | If the Police are requesting information without consent of the Data Subject it should be accompanied by a Form 29(3) Data Protection Form. You should escalate the request to the CEO/xxxxxxx |
| Parent or person with parental responsibility | ✓ | Anyone with parental responsibility has the right to request information held about their child. Remember the guidance re the child’s ability to give consent. |
| 🗶 | Should be withheld when it conflicts with the child’s best interest. If a child has said something in the expectation it will not be disclosed then consider if it is in the child’s best interest to disclose it. |
| ✓ | Child age 16 or 17 – The law regards young people age 16 or 17 to be adults for the purpose of rights of confidentiality |
| ? | Children under 16 – consider capacity or seek advice regarding this. |
| Who has parental responsibility? | ✓ | Biological mother |
| ✓ | Biological father **if** Married to the mother at the time of conception or birthMarried the mother after the birth of the child or for babies born since 2003, jointly registered the birth of the baby with the mother |
| ✓ | Unmarried father **if**The child was born after 01/12/2003 and the birth was registered by both parentsThe child was born before 01/12/2003 and a legal agreement can be evidenced with the motherParental responsibility order can be evidenced |
| ✓ | Adoptive parents once order has been made |
| ✓ | Step-parents if a court has provided a parental responsibility order or they have written consent of one of the parents |
| ✓ | Civil partners if they were civil partners at the time the information was provided to/from the child. You should recheck this at the time of the request |
| ✓ | Non civil partners ifThe birth was registered jointlyParental responsibility has been obtained |
| ✓ | Separated people can still have parental responsibility and can request information held about their child but must provide evidence of parental responsibility as per guidance |
| A representative of the Data Subject when the Data Subject lacks capacity | ✓ | Person with authority under Personal Welfare Lasting Power of Attorney withEvidence of authorityEvidence of appointmentEvidence of identityReason for requestExactly (dates or subject) what information is being requested |
| ✓ | Court appointed Deputy with specific welfare responsibilities withEvidence of authorityEvidence of appointmentEvidence of identityReason for requestExactly (dates or subject) what information is being requested |
| ✓ | An appointed independent Mental Capacity Advocate withEvidence of authorityEvidence of appointmentEvidence of identityReason for requestExactly (dates or subject) what information is being requested |
| ? | What can be requested?Information to enable the person to make an informed welfare decision when the Data Subject is unable to do so. This may not include all information held and should be limited to the information required to fulfil their duties under the Mental Capacity Act. |
| Deceased Person’s representative | ✓ | The Data Subject’s executor is the only person who has an unqualified right to access to a deceased person’s information and need give no reason why they require the information |
| ? | Individuals with a claim arising from the Data Subject’s death. This claim may be financial. The responsibility lies with our organisation to determine if the information we hold would relate to any claim being made by the requestor. Further advice should be sought if necessary and all requests of this nature escalated to xxxxxxxxxxxxxxx |
| Government Benefit Agencies | ✓ | Requests for information may be made by any Government Benefit Agency, Department of Works and Pensions, Criminal Injuries Compensation Authority, Housing etc. however written consent from the Data Subject is required in order to be able to release information |