SUBJECT ACCESS REQUEST POLICY

May 2018

CONTENTS

1 INTRODUCTION

General

1.1 Individuals have the right under data protection legislation (see 2.1), subject to certain exemptions, to have access to their personal data as held by the Royal Free Charity (RFC). This is known as a 'subject access request' (SAR). Requests may be received from supporters, service users, employees or any other individual with whom the RFC has had dealings 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.

1.2 The RFC has developed this policy to guide employees when dealing with Subject Access Requests that may be received.

2 POLICY STATEMENT

The RFC has a duty as a data controller to respect the rights of individuals to access their personal data. These rights and duties are set out in the General Data Protection Regulation (Regulation (EU) 2016/679) and are often referred to as 'the right of subject access.' The Royal Free Charity aspires to comply with the regulation and all Royal Free Charity employees is required to comply with this policy.

3 SCOPE

This policy applies to those members of staff that are directly employed by the RFC and for whom the RFC has legal responsibility. For those staff covered by a letter of contract or work experience the charity's policies are also applicable whilst undertaking duties for or on behalf of the RFC. Further, this procedure applies to all third parties and others authorised to undertake work on behalf of the RFC.

4 POLICY PURPOSE / AIMS AND FAILURE TO COMPLY

4.1 The aim of this policy is to inform staff regarding the nature of subject access requests, how to recognise a subject access request and know what action to take on receipt.

4.2 This policy sets out the process to be followed to respond to a subject access request. This is based on the Information Commissioner's Office Subject Access Code of Practice: https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

5 PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS

General Data Protection Regulations

5.1 Under GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information (this largely corresponds to the information that is referenced to in the RFC's Privacy Policy.

6 ROLES / RESPONSIBILITIES / DUTIES

Responsible Officer
The Responsible Officer for RFC is the Data Protection Lead who has overall responsibility for the Subject Access request Policy within the RFC.

6.1 All Subject Access Requests will be reviewed by the Data Protection Lead to decide to what extent data can be disclosed or whether in exceptional circumstances the request is to be refused.

Employees
All employees are responsible for supporting the fulfillment of the responsibilities of the Data Controller (RFC) and for appropriately signposting requests promptly to enable the RFC to comply with statutory time limits.

Contracts, Contractors and their Employees
Where personal data is processed by a third party on behalf of RFC they are required to support RFC in discharge of its duties.

7 WHAT IS A SUBJECT ACCESS REQUEST?

7.1 A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by the RFC. GDPR entitles all individuals to make requests about 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).

7.2 The request does not have to be in any particular form other than in writing, nor does it have to include the words 'subject access' or make any reference to GDPR. A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way. The applicant must be informed of how the application is being dealt, under which legislation and free of charge, except where the request is manifestly unfounded or excessive.

7.3 Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. Subject access, however, goes further than this and an individual is entitled to be:

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

7.4 Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. The 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.

8 HOW TO RECOGNISE AND ACTION A SUBJECT ACCESS REQUEST

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

- The request must be made in writing (this may be by letter, email or even social media, such as Facebook or Twitter). It is important to note that responses to SAR requests must be returned by a secure medium, 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 applicant's file.
- fees can only be levied where the request is deemed manifestly unfounded or excessive.
- 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).
- Sufficient information to be able to locate the record or information requested. All requests must be responded to without delay and at the latest within 30 days of receipt of the request. This time can be extended by a further two 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. Failure to do so is an offence under GDPR.

8.2 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 FOI request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under GDPR, and another for the remaining, non-personal information made under FOIA.

8.3 Any requests made for non-personal information must be forwarded to the Chief Executive's office. It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA to the world at large, this could lead to a breach of GDPR principles.

8.4 All SAR requests received must be forwarded to the Data Protection Lead, who will record the request and liaise with staff in the appropriate department, e.g. requests to access to personnel records will be sent to the Head of HR. Any SAR received by other employees must be forwarded to the Data Protection Lead without delay in order for the request to be processed within the legal timescale.

8.5 Were the RFC is to process a large quantity of information about an individual, GDPR permits RFC to ask the individual to specify the information the request relates to.

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

8.7 Where requests are manifestly unfounded or excessive, in particular because they are repetitive, RFC can:-

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

Where RFC refuses to respond, it must explain the decision to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy

without undue delay and at the latest within one month.

9 ASSISTING AND ADVISING INDIVIDUALS ON HOW TO MAKE A REQUEST

9.1 If individuals make the request verbally, they need to be advised that they will need to:

- Put the request in writing, detailing the information they are requesting and, if appropriate from which department, in order to enable the data to be located.
- Requesters do not have to tell us their reason for making the request or what they intend to do with the information requested, although it may help RFC to find the relevant information if they do explain the purpose of the request.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure that all Charity employees (including its subsidiaries) can recognise a SAR and deal with it in accordance to this policy and forward immediately to the Data Protection Lead.
- Send the request to the appropriate person (Data Protection Lead) and provide contact details.
- Where an applicant is unable to put the request in writing due to a disability, assistance should be given to them to make the request verbally. Best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct.

Note: responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g. braille.

10 REQUESTS MADE ABOUT OR ON BEHALF OF OTHER INDIVIDUALS

General Third Party

10.1 A third party, e.g. solicitor, may make a valid SAR on behalf of an individual. If, however, a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individual's 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.

10.2 If the Data Protection Lead thinks that an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, the response may be sent directly to the individual 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 in respect of Crime and Taxation e.g. from the Police or HMRC

10.3 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.

10.4 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.

10.5 These types of requests must be considered carefully and the decision on whether to share the information or not be documented before any action is taken. Advice may need to be sought from the Information Commissioner Office.

Court Orders

10.6 Any court order requiring the supply of personal information about an individual must be complied with.

11 RESPONDING TO REQUESTS

11.1 It is essential that a log of all requests received be maintained. It must include:

- Date received
- Date response due (within one calendar month of receipt unless complex case)
- Applicant's details
- Details of information requested
- Indication of whether the request is to be treated as a routine enquiry or as a subject access request
- If applicable, exemptions applied in respect of information not to be disclosed
- Details of any decisions to disclose information without the data subjects consent
- Summary of the information to be disclosed and the format in which it was supplied
- Link to the appropriate folder where copy of the information supplied is kept (password secured)
- Date when information was supplied and how (e.g. paper copy and postal method used for sending)

11.2 The following are likely to be treated as formal subject access requests:

- Please send me a copy of my HR file
- I am a solicitor acting on behalf of my client and request a copy of his records in your database
- A request by the Police stating that they are investigating a crime and they provide an appropriate form requesting the information and signed by a senior officer

11.3 Ensure that adequate proof of the identity of both the data subject and the applicant, where this is a third party, is obtained before releasing information requested.

11.4 Ensure that adequate information has been received to facilitate locating the information requested. The required information will be sought from all appropriate locations and collated for review by the Data Protection Lead. The review will ensure that the information is appropriate for disclosure and that exemptions do not apply (e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed, or it is information to be withheld due to on-going formal investigations). Advice may be sought from solicitors or the Information Commission Office. Exemptions are detailed in Appendix 2.

11.5 In the case of requests for clinical records, the applicant must be informed that they

should contact The Royal Free London NHS Foundation Trust as the Royal Free Charity does not keep any clinical records on subjects.

11.6 Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual.

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

11.8 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.

11.9 It must be determined whether the information is likely to change between receipt of request and its supply. Routine on-going additions and amendments due to normal business practice 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 GDPR.

11.10 Check whether the information collated contains any information about any other individuals. If so, the following must be considered:

11.10.1 Is it possible to comply with the request without revealing information that relates to a third party? We must ensure that any information given does not identify the third party.

11.11 Where it is not possible to remove third party identifiers, the following must be considered:

11.11.1 Has the third party consented to the disclosure?

11.11.2 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 obtain consent from third party,
- whether the third party is capable of giving consent

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

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

11.12.1 Crime prevention and detection, including taxation purposes,

11.12.2 Negotiations with the requestor,

11.12.3 Management forecasts,

11.12.4 Confidential references given by you,

11.12.5 Information used in research, historical or statistical purposes; and

11.12.6 Information covered by legal professional privilege.

11.13 Other exemptions are detailed at Appendix 2

11.14 If the information requested is held by the charity and exemptions apply, then a decision must be made as to whether the applicant is informed that the information is held but exempt from disclosure or whether a reply is sent stating that no relevant information is held. A response in these circumstances must be considered very carefully and applied as appropriate after giving due consideration to the exemptions being applied as it may be appropriate to deny access to information held if the disclosure would prejudice on-going or potential investigations or cause undue harm or distress. *NB* it may be necessary to reconsider this decision should a subsequent application be made and the circumstances around the use of exemptions have changed.

11.15 If the information contains complex terms or codes, the charity must ensure that these terms and codes are explained in such a manner that the information can be understood by lay persons.

Preparing the Response

11.16 When the requested information is not held by the charity we will inform the applicant as soon as possible, but in any case no later than 30 days after receiving request.

11.17 The information will be supplied in a format agreed with the applicant. If the request is received electronically, the response will be sent in an electronic format. There are 30 days to respond to SARs and it is an offence under GDPR not to respond within this time limit.

11.18 Under no circumstance should original records be sent to the applicant.

11.19 The information supplied will be reviewed by the Data Protection Lead and by one other Senior Manager of the Charity. Records must be kept of any written authorisation or agreement for exemptions applied for disclosure or non-disclosure of the information.

12 POLICY IMPLEMENTATION

12.1 Following approval by the Senior Management Team and the Board of Trustees, the policy will be sent to all staff via the electronic HR system.

13 TRAINING AND AWARENESS

13.1 This policy will be published on RFC's electronic HR system and employees will be briefed at departmental meetings. Any amendments to this policy will be also be brought to the attention of employees at those meetings, plus alerts through the electronic HR system.

13.2 The policy will be brought to the attention of all new employees as part of the induction process.

14 POLICY REVIEW

14.1 This policy will be reviewed on an annual basis. Earlier review may be required in response to exceptional circumstances, organizational change or relevant changes in legislation or general practice guidance.

15 CONTACT DETAILS

Data Protection Lead Telephone: 020 7317 7774
Email: rf.charityinfo@nhs.net

16. Appendix 1
Registration and Authentication Examples of Documentary Evidence

Applicants will be requested to supply one from each of the following categories of documents (The Royal Free Charity reserves the right to see the original document and not just a copy)

Personal identity

- Current signed passport
- Residence permit issued by Home Office to EU Nationals on sight of own country passport
- Current UK photo card driving licence
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the right to benefit
- Recent Inland Revenue tax notification
- Building industry sub-contractor's certificate issued by the Inland Revenue
- 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)
- Home Office letter IS KOS EX or KOS EX2
- Police registration document
- HM Forces Identity Card

Active in the Community

These documents should be recent, not more than six months old unless there is a god reason why not, and should contain the name and address of the applicant.

- 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. Please note that mobile telephone bills are not accepted as they can be sent to different addresses and bills printed from the internet may 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)
- 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 of work & Pensions confirming the rights to benefit
- Court order

17. Appendix 2
Subject Access Request Exemptions

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
Social Work	Where the 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 person2 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
Confidential references	We do not have to provide subject access to references we have confidentially given in relation to an employee's employment
Management information	Personal data which relates to management forecasting or planning (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation)
Legal Professional Privilege	Any correspondence to or from or documentation prepared for or by the Charity's internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information
Settlement negotiations	The subject is not entitled to personal data which consists of a record of the employers intentions in respect of settlement discussions that have taken place or are in the process of taking place with that individual
Intellectual property	Subjects are not entitled to information regarding intellectual property rights and trade secrets as these need to be protected

This is not an exhaustive list as there is no comprehensive list in the regulation.

Version Control Sheet

Version	Date	Author	Status	Comments
1	May 2018	Data Protection Lead	Approved	To be reviewed annually, forms part of the Data Protection group