



Data Subject Access Request Policy & Procedure

At a glance

This policy explains how we handle requests for access to personal data under the data protection legislation and what you should do if you receive a request.

Who this policy applies to

This policy applies to all members of staff who work under a contract of employment with Harry's Rainbow, volunteers and to members of the Board.

Policy status

This policy is owned by the Board of Trustees. It is non-contractual and may be updated or changed by the Board at any time. The Board will take steps to ensure that staff, volunteers and board members are provided with an updated version of this policy at any point it is amended.

Staff, volunteers and board members are required to provide a signed copy of this policy to their line manager/supervisor or the CEO as appropriate at any amendment point to evidence they understand the document and any changes made.

Introduction

This Policy sets out the obligations of Harry's Rainbow, a registered Charity in the United Kingdom under number 1194917, whose registered office is at Milton Keynes business Centre, Hayley Court, Linford Wood, MK14 6GD ("the Charity") regarding data subject access requests under the Data Protection Legislation (defined below).

This Policy also provides guidance on the handling of data subject access requests. The procedures and principles set out in this document must be followed at all times by the Charity, its employees, agents, contractors, volunteers or other parties working on behalf of the Charity.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

Data Protection Lead & Scope of Policy

The Charity's Data Lead is Odette Mould, odette@harrysrainbow.co.uk.

The Data Protection Lead is responsible for:

- administering this Policy;
- for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines;
- for ensuring that all data subject access requests are handled in accordance with the Data Protection Legislation.

The Charity collects, holds, and processes personal data about clients, employees, volunteers, supporters and business contacts. The Charity is a 'data controller' for the purposes of the Data Protection Legislation.

Data subjects have rights with respect to their personal data under the Data Protection Legislation.

This Policy deals specifically with the right of access but the procedural elements will also explain our approach to other rights requests. .

Data subjects have the right to find out whether the Charity collects, holds, or processes personal data about them, the right to request a copy of any such data, and other supplementary information. The right of access is designed to help data subjects to understand how and why we use their data, and to check that we are doing so lawfully.

This Policy should, be read in conjunction with the Charity's Data Protection Policy and Data Retention Policy.

Any questions relating to this Policy, the Charity's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Lead.

Parts 1 to 4 and Parts 14 to 16 of this Policy apply to all staff and any other party acting on behalf of the charity and Parts 5 to 13 apply to staff authorised to handle data subject access requests.

How to Recognise a Data Subject Access Request

The Data Protection Legislation does not set out a particular format which a data subject access request (hereafter "SAR") must follow. A SAR may be made orally or in writing, to any part of the Charity, and by any means of communication.

A SAR does not need to use the words 'subject access request', 'data protection', 'personal data' or similar terms, or refer to Article 15 of the GDPR. This means that anyone in the Charity could receive a SAR and it may not be immediately obvious that a SAR has been received.

The Charity provides a Subject Access Request Form, available from the shared drive, to make it easier for data subjects to make a SAR and to make it easier for the Charity to recognise the request; however, data subjects are under no obligation to use the form and care must be taken at all times to identify SARs made in other ways.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

SARs may instead use more general terminology, using terms such as ‘information’ rather than ‘personal data’. For example, a message sent to the Charity via social media such as ‘please provide details of all the information you have about me’ will be a valid SAR and must be treated in the same way as a more formal communication using our SAR Form referring specifically to a ‘subject access request’ and data subjects’ rights under the GDPR.

Individuals may make SARs on their own behalf. It is also possible to make an SAR via a third party:

This may be a solicitor making a request on behalf of a client, or it may be one private individual making the request on behalf of another. This is permissible, but you must be satisfied that the individual making the request has the authority to act on behalf of the data subject concerned.

In certain limited cases, an individual may not have the mental capacity to manage their own affairs. In these cases, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of that individual.

Adults, such as parents or guardians, may make SARs on behalf of children. The right of access itself, however, remains the child’s right. When dealing with a SAR about a child it is important to consider whether that child is mature enough to understand their rights. If so, a response directly to the child should be considered. It may, however, be permissible to allow the adult to exercise the child’s right on the child’s behalf if the child has given their authorisation, or if it is evident that doing so is in the child’s best interests.

When a SAR is identified, or if a communication or request is received and you are in anyway unsure whether or not it is a SAR, it should be immediately forwarded to the Charity’s Data Protection Lead as set out below.

What to do When a Subject Access Request is Received

The Charity has a limited timeframe within which to respond to a SAR, so it is important to act quickly.

Unless you are authorised to handle a SAR, it must be forwarded to the Data Protection Lead immediately. Please do not take any further action with respect to any SAR unless you are authorised to do so.

SARs may come in any form. This will determine how to forward the SAR to the appropriate member of staff:

For SARs received by email or via social media, the message or a link, if appropriate must be forwarded immediately to the Charity’s Data Protection Lead.

For SARs received by post or in any other hardcopy form, the SAR should first be scanned and emailed immediately to the Charity’s Data Protection Lead, and the original sent to the same recipient using the most direct and secure means possible (e.g. in person, by courier if available, or by Royal Mail Special Service).

For SARs made verbally, the name and contact details of the data subject should first be recorded before informing the data subject that the Charity’s Data Protection Lead will contact them for full details of their SAR. The data subject’s details and any other information provided by the data

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

subject should be emailed immediately to the Data Protection Lead, including details of the time and date on which the SAR was made.

The Charity's Data Protection Lead should respond to you, confirming receipt of the SAR, within 2 business days of you sending it. If you do not receive a response within this period, you must contact them again to confirm receipt.

Responding to a Subject Access Request Part 1: Identifying Data Subjects and Clarifying Requests

Before responding to a SAR, all reasonable steps must be taken to verify the identity of the individual making the request and, if the Charity is processing a large amount of personal data about them, to clarify their request (i.e. to specify the personal data or processing to which their SAR relates). Information requested for such purposes must be reasonable and proportionate. Individuals must not be asked to provide any more information than is reasonably necessary.

If additional information is required to confirm an individual's identity, the individual must be informed as soon as possible. If additional information is required, the time limit for responding to a SAR does not begin until that information is received.

If additional information is required to respond to the SAR, the individual must be informed as soon as possible. For example we have more than one John Smith please can you provide your date of birth for us to be sure which John is requesting their records

This is different from refining a search. If we cannot proceed without the extra information, then the time limit for response does not start until we have received that additional information.

However, that if additional information is requested to refine or limit our searches, the time limit for responding to a SAR is not affected and a response must still be given within one month of receipt of the SAR (subject to the possible extensions to the time limit explained below).

If a SAR is made by a third party on behalf of a data subject, the individual acting on behalf of the data subject is required to provide sufficient evidence that they are authorised to act on the data subject's behalf.

Examples of information that may be requested to confirm an individual's identity include:

- A copy of the individual's passport;
- A copy of the individual's driving licence;

If, having requested additional information to verify an individual's identity, it is still not possible to do so (if, for example, the individual does not comply), the Charity may refuse to comply with a SAR,.

If, having requested additional information to refine a SAR, the individual does not comply, the Charity must still endeavour to comply with the SAR by making reasonable searches for the personal data relating to the request.

The Charity does not retain personal data for the sole purpose of being able to respond to a potential SAR.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

Responding to a Subject Access Request Part 2: Fees

Under normal circumstances, the Data Protection Legislation prohibits the charging of a fee for handling a SAR. The Charity does not normally charge for SARs.

In limited cases, it is permissible to charge a 'reasonable fee' in order to cover the administrative costs of complying with a SAR if that SAR is 'manifestly unfounded', 'excessive', or if a data subject requests further copies of their data following the SAR. In certain cases, it may also be permissible to refuse to comply with a SAR.

Responding to a Subject Access Request Part 3: Time Limits

Under normal circumstances, the Charity must respond to a SAR 'without undue delay' and, at the latest, within one month of receipt. The date of receipt of all SARs must be recorded, along with the due date for response.

Under the Data Protection Legislation, the one-month period referred to in Part 8.1 begins on the calendar day – not business day – after the request is received and ends on the corresponding calendar day in the following month (or, if the following month is shorter and does not have a corresponding day (e.g. January 31st to February 28th), the last day of that month). Consequently, the time limit set by the Charity for responding to SARs is 28 calendar days. If the last day of the time limit falls on a weekend or bank holiday, the time limit is extended to the next business day.

If additional information is required from the individual making the SAR to confirm an individual's identity, the time limit begins on the day that this information is received.

If additional information is required from the individual making the SAR to refine the SAR, the time limit is unaffected and begins on the day that the SAR is received, providing it is valid.

If the SAR is complex, or if the same data subject makes a number of SARs, it is permissible to extend the time limit by up to two months. If such an extension is necessary, the data subject must be informed, in writing, of the reason(s) for the extension within the original one-month time limit.

Responding to a Subject Access Request Part 4: Information to be Provided

In addition to a copy of the personal data held by the charity, data subjects must be provided with the following information in response to a SAR:

- the purposes for which the Charity collects, holds, and processes their personal data;
- the categories of personal data involved;
- the recipients or categories of recipient to whom the Charity discloses their personal data;

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

- details of how long the Charity retains their personal data or, if there is no fixed period, our criteria for determining how long it will be retained;
- details of the data subject’s right to ask the Charity to rectify or erase their personal data, or to restrict or object to our processing of it;
- details of the data subject’s right to make a complaint to the ICO or to another supervisory authority;
- if any of the personal data in question was not obtained from the data subject, details of the source of that data;
- if the Charity carries out any automated decision-making (including profiling), details of that automated decision-making, including a meaningful explanation of the logic involved and the significance and envisaged consequences for the data subject (also see Part 9.2); and
- if the Charity transfers their personal data to a third country (i.e. non-EEA) or international organisation, details of the safeguards in place to protect that data.

The information set out above must be provided:

- in clear plain easy to read language;
- in writing; and
- if the data subject has made the SAR electronically, in a commonly-used electronic format (unless the data subject requests otherwise); and
- where possible, by using the Charity’s secure portal system, providing secure access for data subjects to their personal data.

It is important to note that data subjects are only entitled to access personal data that the Charity holds about them. If information located in the process of responding to a SAR does not meet the definition of “personal data” the Data Protection Legislation does not entitle the data subject to access it. In certain cases, it may be necessary to separate personal data from non-personal data when responding to a SAR.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

Responding to a Subject Access Request Part 5: Locating Information

The Charity holds personal data in the following locations and/or systems. It is important to identify the type(s) of personal data to which a SAR relates in order to search in the correct place:

- Email;
- Client Management system;
- Paper documents.

Refusing to Respond to a Subject Access Request

In certain cases, it is permissible for the Charity to refuse to comply with a SAR: if it is not possible to identify the individual making the SAR after requesting additional verification; or

if the request is 'manifestly unfounded' or 'excessive', taking into account whether the request is repetitive in nature. In such cases, it is also possible to request a 'reasonable fee' to handle it.

If either of the above grounds applies, the Charity's refusal to comply with the SAR must be justified and an explanation must be provided to the individual making the SAR within one calendar month after receiving the SAR. The individual must also be informed of their right to complain to the ICO or another supervisory authority and of possibility of seeking a judicial remedy.

Certain exemptions to the right of access are also included in the Data Protection Legislation.

Exemptions to the Right of Access

The Data Protection Legislation provides a number of exemptions which apply to SARs and therefore justify the Charity refusing to comply with a SAR. Those most likely to be applicable within the Charity are situations in which the personal data in question is:

- subject to legal or litigation privilege; or
- a reference given (or to be given) in confidence for purposes of employment, training, or education; or
- is processed for management forecasting or management planning purposes in relation to a business or other activity (but only to the extent that complying with the SAR would prejudice the conduct of the business or activity); or
- consists of records of intentions with respect to negotiations between employer and employee (but only to the extent that complying with the SAR would prejudice such negotiations); or
- contains personal data concerning a third party; or
- is of a type likely to prejudice the prevention or detection of a crime, or the apprehension or prosecution of offenders if it is disclosed.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026

Additional exemptions relate to more specific (and generally public) matters such as national security. If any concerns or questions arise with respect to exemptions which may or may not apply during the process of handling a SAR (including, but not limited to those set out above), those questions should be referred to the Charity's Data Protection Lead and/or to the ICO.

Failure to Comply with this Policy

Compliance with the Data Protection Legislation is of vital importance to the Charity. If we fail to comply with a SAR within the required time limit or fail to provide a data subject with access to the personal data that we hold about them, we will be in breach of our obligations under the Data Protection Legislation.

Failing to comply with the Data Protection Legislation may put the data subject at risk. It may also result in the following consequences for the Charity:

- the data subject reporting the Charity to the ICO, resulting in an investigation by the ICO;
- enforcement action taken against the Charity which may result in civil and/or criminal sanctions for the Charity and, in certain cases, the individual responsible for the breach;
- if the data subject has suffered damage and/or distress as a result of the Charity's breach, the data subject may seek further legal remedies such as damages against the Charity; and
- a court may order the Charity to comply with the SAR in any event if the Charity is found to have failed in its compliance with the Data Protection Legislation.

Failure by any member of staff to comply with this Policy may result in disciplinary action which may include dismissal for gross misconduct.

Policy Review

This Policy will be reviewed on a yearly basis. The Charity's Data Protection Lead shall be responsible for reviewing this Policy.

Implementation of Policy

This Policy shall be deemed effective as of 20th December 2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Owner: Odette Mould	Approved/Reviewed Date: 02/10/2024
Approved by: The Board	Review Date: 02/10/2026