Coles', Moorpool & The Eyre St Thomas Day Charity Subject Access Policy (SAR) and template response letters

Subject Access Requests ("SAR") Checklist

A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).

B. Make sure a SAR policy is in place within the Charity and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:

(1) Responsibilities (who, what)

(2) Timing

(3) Changes to data

(4) Handling requests for rectification, erasure or restriction of processing.

C. Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

D. Where possible, implement standards to respond to SARs, including a standard response.

1. Upon receipt of a SAR

(a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. Responding to a SAR

(a) Respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the Charity cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses[2];

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data;

(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Provide a copy of the personal data undergoing processing.

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to [ ]
2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation
3. ***MUST***: A member of staff, and as appropriate, trustee, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.
4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.
6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. ***MUST***: trustees and managers must ensure that the staff they manage are **aware** of and follow this guidance.

[1] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation's headquarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[2] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the charity must manage this as a **complaint**.

How must I do it?

1. Notify [ ] upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the charity relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The charity accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):
    - Current UK/EEA Passport
    - UK Photocard Driving Licence (Full or Provisional)
    - Firearms Licence / Shotgun Certificate
    - EEA National Identity Card
    - Full UK Paper Driving Licence
    - State Benefits Entitlement Document*
    - State Pension Entitlement Document*
    - HMRC Tax Credit Document*
    - Local Authority Benefit Document*
    - State/Local Authority Educational Grant Document*
    - HMRC Tax Notification Document
    - Disabled Driver's Pass
    - Financial Statement issued by bank, building society or credit card company+
    - Judiciary Document such as a Notice of Hearing, Summons or Court Order
    - Utility bill for supply of gas, electric, water or telephone landline+
    - Most recent Mortgage Statement
    - Most recent council Tax Bill/Demand or Statement
    - Tenancy Agreement
    - Building Society Passbook which shows a transaction in the last 3 months and your address
3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear on forms and on the charity website

6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database is maintained allowing the charity to report on the volume of requests and compliance against the statutory timescale.

8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

E. Sample letters

3. All letters must include the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[3] or EU model clauses[4];

(d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(g) if the data has not been collected from the data subject: the source of such data;

(h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4. Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the charity or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

5. Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

[3] "Binding Corporate Rules" is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[4] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the charity or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwisemade available in whole or in part without the prior written consent of the copyrightholder.

Yours sincerely"

6. Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example, the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the charity or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the charity is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the charity should set out the reason why some of the data has been excluded.]

Yours sincerely"