RCS

RCS Subject Access Request Policy

This policy and procedure concerns people's rights under the General Data Protection Regulation to access the personal data held about them by RCS and its funding partners. Specifically it refers to the data subject's right of access to the information held on them and the right to be informed about how their personal information is processed after they have shared it with RCS.

It is the responsibility of everyone within RCS to respond quickly and appropriately when any of our data subjects requests a copy of the information RCS holds on them.

The attached procedure is a guide to the steps that will need to be taken when a subject access request is received.

What is personal data?
Under GDPR 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What is a Subject Access Request (SAR)?
A subject access request (SAR) is simply a written request made by *or on behalf of* an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA). The right of access is continues under the General Data Protection Regulations with certain changes.
The request should be in writing but does not have to be in any particular form.

Our responsibilities in responding to a SAR.

1. Subject Access Requests must be undertaken free of charge (in some conditions the legislation permits reasonable fees to be charged but this would be unusual).
2. In responding to a SAR we will need to search all the 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 we are responsible for or we own.
3. We must not withhold personal data simply because we believe it will be misunderstood. Instead, we must provide an explanation with the personal data so the data subject can understand.
4. We must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and any complex terms used.
5. 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. RCS may however be able to agree with the requester that they will view the personal data on screen or inspect files on our premises.
6. We must redact any exempt unrelated personal data from the released documents and explain why that personal data is being withheld.
7. We must respond to a SAR within one calendar month after accepting the request as valid. If more time is needed (e.g. to respond to complex requests) an extension of

another two months is permissible, provided we have communicated this to the data subject in a timely manner within the first month.

8. If RCS cannot provide the information requested, it should inform the data subject without delay and at the latest within one month of receipt of the request.
9. RCS must keep records of the SAR and any changes that occur to the data as a result.
10. We must ensure that the data subject is asking for sufficiently well-defined personal data held by RCS relating to the data subject.
11. We should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity.

Our responsibilities following completion of a SAR

After RCS has responded to a SAR, we must recognize that the data subject has further rights. They have a right to have any data, corrected, updated or erased.

The data subject may also object to having their data processed in certain ways. RCS must respond promptly to the data subjects concerns and restrict processing as directed.

A record must be kept of any alterations made to the data as a result of a request by the data subject to do so.

Complaints

The data subject may complain to the Information Commissioner if they feel RCS has failed to remedy inaccuracies in their personal data and processes. Details of how they can do this are made publically available in the RCS privacy notices which accompany an initial consent giving and which are publically available on the RCS website.

Record keeping

A SAR spreadsheet is maintained allowing RCS to report on the volume of requests and compliance against the statutory timescale.

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.

Date Ratified by RCS Board	28 March 2018
Effective From	28 March 2018
Review Date	March 2021
Policy Owner	Data Protection Officer

RCS

RCS Subject Access Request Procedure

On receipt of a Subject access request

On receipt of a subject access request RCS will verify whether RCS is the controller of the data subject's personal data. This will be done by checking the terms of the contract under which the OPAL service is performed. If RCS is not a controller but a processor, the data subject will be informed by the Organiser and referred to the actual controller. The Data Protection Officer will pass the subject access request on to the data controller**.**

Where RCS is the data controller:

1 On receipt of a subject access request you must immediately inform the Organiser and the Data Protection Officer (or another Trustee).
2 The Organiser will promptly acknowledge receipt of the SAR in writing.
3 On receipt of the SAR the Organiser will record receipt and acknowledgement of the SAR
4 The Organiser will verify the identity of the data subject and if needed, will request any further evidence on the identity of the data subject.
5 The Data Protection Officer will correctly identify whether a request has been made under the Data Protection legislation.
6 The Organiser and the Data Protection Officer will verify if the access request is sufficiently substantiated. i.e. Is it clear to the data controller what personal data is requested? If not, additional information will be requested.
7 The Organiser will verify whether we process the data requested. If we do not possess any data, the Organiser will inform the data subject accordingly.
8 The Organiser will locate and supply personal data relating to the SAR. The Organiser, with help from the Administrator, must make a full exhaustive search of all records to which RCS has access. This includes emails. All the personal data that has been requested must be provided unless an exemption can be applied. Where necessary the Organiser will alert other staff and Trustees about the SAR and request any records held by others will be made available promptly and without delay.
9 All data processors will ensure that no data is changed as a result of the SAR. Only routine changes as part of the processing activities concerned are permitted.
10 The Organiser and Data Protection Officer will verify whether the data requested also involves data on other data subjects. Where this is the case, this data must be filtered before the requested data is supplied to the data subject. If data cannot be filtered or redacted, other data subjects identified must consent to the supply of their data as part of the SAR.
11 At all times the Organiser together with the Data Protection Officer will make sure the internal SAR policy is followed and progress can be monitored.

Responding to a SAR

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

- the purposes of the processing.
- the categories of personal data concerned.
- the recipients or categories of recipients to whom personal data has been or will be disclosed, especially if it has been disclosed to international organisations, including

any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses.

- where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.
- 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.
- the right to lodge a complaint with the Information Commissioner's Office (ICO).
- if the data has not been collected from the data subject: the source of such data.
- 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.
- Provide a copy of the personal data undergoing processing.

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