# Data Subject Rights Procedures

December 2019

www.southglos.gov.uk

South Gloucestershire Council

# Version history

This document contains and replaces March 2014 edition

| Version | Date | Amendments |
|---|---|---|
| 1 | 2003 | First edition |
| 2 | February 2013 | Second edition (complete review of first edition) |
| 3 | August 2013 | Version 2.3 (request for Subject Access Request(SAR) review added) |
| 4 | March 2014 | Version 2.4 (improved format and contact details updated) |
| 5 | August 2018 | Version 2.5 (reviewed in light of GDPR and further detail added in respect of exemptions and process) |
| 6 | January 2019 | Version 2.6 (as above following the ICO exemptions guidance being published) |
| 7 | June 2019 | Version 2.7 (as above but title changed to reference wider data subject rights than solely subject access. The ICO guidance for organisations aligns consideration of other requests from data subjects (e.g. the right to object, erasure, rectification) with the process for considering data subject access requests). |
| 8 | December 2019 | Version 3.0 Final version following the council's Data and Information Group (DIG) review |
| | | |

## Table of contents

# PART ONE: DATA SUBJECT RIGHTS REQUEST PROCEDURES

## 1. Introduction

This document sets out the council's procedure for managing requests by data subjects exercising their rights as set out in the Data Protection Act 2018 and The General Data Protection Regulation (GDPR) (EU) 2016/679. Individuals whose data is being processed (data subjects) have the following rights under this legislation:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure or 'right to be forgotten'
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights on automated decision making and profiling

Part one of this document provides an overview of data subject rights and the procedures for managing these. Part two provides more detailed information in relation to managing data subject access requests.

## 2. Who are 'data subjects'?

A data subject refers to a living individual who can be identified from information either directly or indirectly. Personal data is the information that relates to the individual. Some records contain personal information about other individuals and it may be difficult to isolate the personal data of specific individuals. The Information Commissioner's Office (ICO) has guidance to help determine what information is personal data.

## 3. Overview of data subject rights

### 3.1 The right to be informed

Individuals have a right to be informed about the collection and use of their personal data. Transparency is a key requirement under the GDPR. Individuals must be provided with information about why their data is being processed, how long their information will be retained for and who it will be shared with. In addition they must be told:

- The name and contact details for South Gloucestershire Council (the data controller) and any processing partner
- The name of the council's Data Protection Officer
- The purpose and legal basis for the processing

This is known as 'privacy information'. Privacy information must be provided to individuals at the time that their data is collected from them. If the data is collected from other sources then they must be provided with the privacy information within

a reasonable time from the time the data was collected and no later than one month.

The privacy information should be concise, transparent, intelligible, easily accessible and it must use clear and plain language. Privacy information must be kept under review and updated as necessary.

The information needs to be informed of:

•

The council's overarching privacy information is available from our website. Services need to be mindful of the specific privacy information they need to provide to individuals.

### 3.2 The right of access

A subject access request (SAR) enables individuals to find out what personal data we hold about them, why we hold it and who we disclose it to.

An individual has the right to access personal information held about them except where:

- it contains confidential information about other people and the council has to balance the rights of other individuals
- includes information a care professional thinks will cause serious harm to them or someone else's physical or mental wellbeing
- information which may prejudice an investigation if disclosed

**What information is an individual entitled to when they request access?**

Subject access requests are most often made by individuals who want to see a copy of the information an organisation holds about them. However, except where an exemption applies subject access entitles an individual 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 any other organisations or people;
- given details of the source of the data (where this is available).

Subject access provides a right to see the personal information, rather than a right to have copies of the documents that include that information. Although the easiest way to provide the relevant information is often to supply copies of the original this is not an obligation.

In some instances the personal data may be exempt from subject access. More information about this is available at section 16.

More detailed information about managing access requests and is available from the subject access request procedures shown below.

3.3 **The right to rectification**

An individual has a right to inaccurate personal data corrected or completed if it is incomplete.

A lead officer will be appointed to consider a request for rectification. They will need to take account the arguments and evidence provided by the individual and take reasonable steps to check the accuracy of the data. Any inaccuracies or incompleteness of the data needs to be corrected as soon as possible.

When considering any rectification of data advice should be sought from the relevant senior manager and information management team. Factually inaccurate information should be corrected however it may be more complex if the data concerns a disputed opinion. It may be difficult to conclude that a record of an opinion is inaccurate and in such instances it may be necessary to make a note next to the record of the objection.

The lead officer should send a response to the individual explaining whether they consider the information to be inaccurate or not. The decision should be clearly explained in the response and informing them of the right to make a complaint to the ICO.

Consideration will need to be given to contacting any third parties that the data was originally shared with. They may need to be advised of any amendment.

3.4 **The right to erasure or 'right to be forgotten'**

An individual can ask for personal data to be erased. The right is not absolute and applies only when:

a) the personal data is no longer necessary in relation to the purposes for which it was collected and processed
b) the council's lawful basis for processing the data was consent and the individual has withdrawn their consent and there is no other legal ground for the processing
c) they object to the data processing and there are no overriding legitimate grounds for processing their data
d) the data has been processed unlawfully or
e) it is necessary for complying with a legal obligation.

A lead officer will be appointed to consider a request for erasure of data.

Consideration will need to be given to contacting any third parties that the data was originally shared with. They will need to be informed of the erasure unless this proves impossible or involves disproportionate effort. If asked to, the individual must be told about these third parties.

The right to erasure doesn't apply if the data processing is necessary for:

a) exercising the right of freedom of expression and information
b) complying with a legal obligation

c) the performance of a task carried out in the public interest or in the exercise of official authority
d) archiving purposes in the public interest or for statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
e) establishing, exercising or defending legal claims
f) public health purposes in the public interest or
g) the provision of health or social care or for the management of health and social care systems or services. This applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional)

### 3.5 The right to restrict processing

An individual can ask for the processing of the personal data to be restricted. This is not an absolute right and only applies in certain circumstances. This right is closely linked to the right to rectification and the right to object. A lead officer will be appointed to consider a request to restrict data processing.

An individual may ask the council to limit the way their information is processed because:

- they may have issues with the accuracy of the information and the council is verifying the accuracy of the data
- they consider the data has been unlawfully processed and rather than asking for the data to be erased ask for it to be restricted instead
- the council no longer needs the information but the individual needs it to be retained in order to establish, exercise or defend a legal claim or
- they have objected to their data being processed and the council is considering whether it has legitimate grounds to override those of the individual.

Advice should be sought from the relevant senior manager, the information management team and any other relevant parties over to how to employ any necessary restriction.

Once the data is restricted it must not be processed except to store it unless:

- the individual has consented
- it is for the establishment, exercise or defence of legal claims
- it is for the protection of rights of another person or
- it is for reasons of important public interest.

The restriction in many cases is only temporary, for example when considering any objections from the individual. Once the decision has been made the restriction may be lifted. The individual must be informed before the restriction is lifted.

3.6 **The right to data portability**

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another is a safe and secure way.

The right to data portability only applies when:

- The individual has consented to the data processing or it is necessary for the performance of a contract and
- The processing is being carried out automatically (i.e. excluding paper files).

Where the information includes information about others consideration will need to be given to whether transmitting the data would have an adverse impact on those third parties. If the information was provided to the council by multiple data subjects it will be necessary to seek the agreement of all the parties involved.

The right entitles the individual to receive a copy of their personal data and / or have their personal data transmitted to a different data controller.

The council needs to consider the technical feasibility of any transmission on a request by request basis and without hindrance. However there may be legitimate reasons why the council cannot undertake the transmission. For example if to do so would have an adverse impact on others. The council must justify its reasons for this to the requester.

3.7 **The right to object**

An individual can object to certain types of processing such as direct marketing. The right to object also applies to other types of processing such as processing for scientific, historical research or statistical purposes (although processing may still be carried out for reasons of public interest).

This right is closely linked to some of the other rights as someone may object to processing and request that certain action is taken (restrict data processing, erasure or rectification or data). A lead officer will be appointed to consider any objections to data processing.

An individual must give specific reasons as to why they object to the data processing. The council can continue processing the data if:

- it can demonstrate compelling legitimate grounds for the processing, which override those of the data subject or
- the processing is for the establishment, exercise or defence of legal claims.

It is important to take account of the reasons given by the individual for their objection. For instance, the processing may be causing them substantial damage or distress. It is necessary to balance the individual's interests and rights against the council's legitimate grounds and to consider whether to stop the processing or not.

A response will need to be provided to the individual advising as to whether the council agrees to stop processing their data or not. The decision needs to be clearly explained.

### 3.8 Rights on automated decision making and profiling

The law provides safeguards for you against the risk that a potentially damaging decision is taken without human intervention. The right does not apply in certain circumstances such as where you give your explicit consent.

For further information on the rights of individuals see the ICO's advice and guidance

## 4. Handling data subject requests

### 4.1 Receiving a request

4.1.1 A request can be made verbally or in writing by or on behalf of an individual. Where the request is made verbally the details should be clarified with the requester to enable a written record of the request to be logged. A copy of this written record should be provided to the requester.

4.1.2 The request does not have to be in any particular form, nor does it have to include the specific words about data subject rights, for example, 'right to object' or 'right to be forgotten' or 'subject access' or make any reference to the Data Protection Act ("the Act"). A request may be a valid request even if it refers to other legislation, such as requesting access to personal information under the Freedom of Information Act. An objection to any data processing may also be referred to as a complaint or a data breach. It is important therefore to seek advice from the departmental FOI team as to the most appropriate procedure to be followed.

4.1.3 A request may be received by any council service and should be logged with the relevant departmental FOI team. The request should be acknowledged and a lead officer appointed to consider the request.

4.1.4 It may be necessary to verify the requester's identity, particularly if someone else is making the request on behalf of the data subject. More information about this is available from sections 4 and 5.

4.1.5 There is no fee to make a subject access request. However where the request is manifestly unfounded or excessive a 'reasonable fee' can be charged for administrative costs of complying with the request. If the individual requests additional copies following a request then an administrative fee to cover copying costs can also be charged.

4.2 **Timescales for responding to data subject requests**

4.2.1 In terms of timescales for responding to data subject requests, in most instances the GDPR says that such request should be responded to without undue delay, except for the right of access which states that these should be responded to within one calendar month. The Information Commissioner's Office (ICO) guidance advises that any data subject request should be responded to within one calendar month. If the request is complex or a number of requests have been received from the individual the ICO advises that the time to respond can be extended by a further two months. The individual must be informed within one month of receiving their request if an extension is required.

4.2.2 The timescale is calculated from the day after receiving the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. For example, if the request is received on 3 September the timescale will start from 4 September. The council therefore has until 4 October to comply with / respond to the request.

4.2.3 If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond. This means that the exact number of days we have to comply with a request varies, depending on the month in which the request was made.

4.2.4 The time to respond can be extended by a further two months if the request is complex or a number of requests from the individual have been received. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

4.2.5 It is not possible to extend the one month time limit on the basis that you have to rely on a data processor to provide the information that you need to respond. The responsibility for responding to a request rests with the council as data controller.

4.3 **Responding to data subject requests**

4.3.1 Responses need to clearly explain the decisions reached and demonstrate the justification for these. The individual needs to be advised of their right to request an internal review of the handling of their request and the council's response. They should also be informed of their right to make a complaint to the ICO as well as their ability to seek to enforce their rights through a judicial remedy.

4.2 **Reviewing responses to data subject requests**

4.3.1 Following the response an individual has the right to go directly to the ICO to complain if they remain dissatisfied with the response provided. They can also ask for an internal review before approaching the ICO. The internal review should be carried out by a more senior manager than the

original lead officer. The reviewer should consider the original request, the response and the information it relates to. The reviewer should also take account of any new information provided by the data subject.

4.3.2 A further response should be provided to the data subject without undue delay. The individual should be advised of the timescale to expect this further response. In calculating a timescale for the review the time taken so far to process the original request should be taken into account.

## 5. Further information

5.1 More information is available from the FOI team on 01454 868009 or freedomofinformation@southglos.gov.uk

# PART TWO: SUBJECT ACCESS REQUEST PROCEDURE

Part two is divided into the following sections:

- Receiving the request
- Processing the request
- Responding to the request

## 6. RECEIVING A SUBJECT ACCESS REQUEST

### 6.1 Key points to consider when receiving a SAR

6.1.1 A subject access request (SAR) may be received verbally or in writing. Where the request is made verbally the details should be clarified with the requester to enable a written record of the request to be logged. A copy of this written record should be provided to the requester. There is a SAR form available from the council's website www.southglos.gov.uk/dataprotection that may help with this. Although the form may make it easier for an individual (the data subject) to ensure they include all the information that we need, there is no requirement for them to use this form.

6.1.2 Requests may also be received via email, fax, letter or social media. If a SAR is received via social media it may be necessary to obtain an alternative means of contact from the individual for the purposes of responding to their request.

6.1.3 Although an individual's request for information may begin in any form such as a verbal conversation it must be followed up with a written request.

6.1.4 Some individuals may struggle to provide a written request and in such circumstances it is reasonable to allow them to make their request verbally. However a written record should be made of the request. When responding

to the request it will be important to consider what support a person may need to understand the information that they have asked for.

6.1.5 Sometimes people wish to request information for themselves and on behalf of someone else, for example a parent. It is important to ensure that you are satisfied that they can make this request. The form also allows official representatives to apply on behalf of another person. See sections 5 for more information.

6.1.6 To avoid personal data about one individual being sent to someone who is not entitled to it, you need to be satisfied that you know the identity of the applicant. Enough information should be requested to confirm the individual's identity; however this must be reasonable especially in situations where the individual is known to the Council through ongoing contact. In such circumstances you may be able to verify the person is who they say they are and can therefore waive the need for them to present proof of identity.

6.1.7 One Stop Shop staff are able to verify identification, copy all the materials/identification and send them onto the departmental FOI team.

6.1.8 All SARs should be sent to the relevant departmental FOI team for recording and monitoring. The contact details for each of the departmental FOI teams is provided at the end of these procedures.

6.1.9 The one calendar month deadline is set by the Act, however in all cases you should respond promptly.

6.1.10 In order to calculate the final deadline the start date is taken as the date that a valid SAR is received. A valid SAR means that the request is clear as the individual has supplied enough information to assist in locating where the information may be held. Section 7 provides further advice on what to do if the request is vague or unclear.

6.1.11 An acknowledgement must be sent to the individual within 2 working days of receipt confirming the timescale for responding to their request. Original identification documents should also be returned with this letter by recorded or registered post.

## 6.2 Requests made on behalf of others

6.2.1 The Data Protection Act (DPA) does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority or might be a more general power of attorney. More information about this is available at in the in section 15 of this document.

6.2.2 When a SAR is received from a law firm, staff must ensure that the request

letter confirms that the council will not be a party to the claim. If the council is a party, the matter should be sent directly to the Risk Management & Insurance Team for their advice. The request letter must also include a signed consent or release form from the client. The information disclosed should be exactly as outlined in the client's consent form. Information must not be released without the client's consent form.

## 6.3 Requests for access to children's information

6.3.1 As a general rule, 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 e.g. to the parent or guardian. So it is the child who has the right of access to the information, even though in the case of young children this is likely to be exercised by those with parental responsibility for them. More information is available in section 15 of this document.

6.3.2 Before responding to a request for information held about a child, you should consider whether the child is mature enough to understand their rights, consideration should be given to consulting with the child and confirming that they are aware of the request. If you are confident that the child can understand their rights, then you should usually respond to the child. However, if the child authorises it or it is evident that it is in the best interests of the child, then the parent can act on their behalf.

6.3.3 What matters is that the child is able to understand (in broad terms) what it means to make a SAR, and to interpret the information they receive as a result of doing so. When considering borderline cases. you should take into account of:

- the child's level of maturity, and their ability to make decisions like this;
- 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;
- any consequences of allowing those with parental responsibility access to the child's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child if this information cannot be accessed by those with parental responsibility; and
- any views the child or young person has on whether their parents should have access to information about them.

6.3.4 In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This presumption does not apply in England, where competence is assessed depending on the level of understanding of the child but it does provide a useful guide.

6.3.5 The exception to this is schools. Under the Education (Pupil Information) (England) Regulations 2005 parents are entitled to have information from

schools records from the school irrespective of the wishes of the child.

## 6.4 Clarifying the request

6.4.1 Where any element of the SAR is unclear it will be necessary to contact the individual again to clarify their request. This may include asking them for information that is reasonably required to find the personal data that they are seeking. We will be unable to comply with the request until this information is received, however there shouldn't be an unreasonable delay in seeking clarification. The timescale for responding starts when the additional information is received. However, if the individual refuses to provide any additional information, we must still endeavour to comply with their request by making reasonable searches.

6.4.2 You cannot ask the individual to narrow the scope of their request but you can ask for more information. For instance, an individual may ask for '*all the information you hold about me*' and they are entitled to make such a request. However you can ask them to provide more information about their contact with the council to enable you to locate the information. This might include, the dates they were in contact with the council, any services they were known to or the names of staff they had contact with. A conversation with the requester may help to clarify their request and therefore avoids unnecessary searches or sending them large amounts of information that they don't want or weren't expecting. Further information about responding to such requests is available within section 15 of this document.

## 6.5 Dealing with repeated or unreasonable requests

6.5.1 The DPA does not limit the number of SARs 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 you are not obliged to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

6.5.2 The DPA gives you some help in deciding whether requests are made at reasonable intervals. It says you should consider the following.

- The nature of the data – this could include considering whether it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause detriment (harm) to the requester.
- How often the data is altered – if information is unlikely to have changed between requests, you may decide that you need not respond to the same request twice.

6.5.3 If there has been a previous request or requests, and the information has been added to or amended since then, when answering a SAR you are required to provide a full response to the request: not merely supply information that is new or has been amended since the last request.

However, in practice we would accept that you may attempt to negotiate with the requester to get them to restrict the scope of their SAR to the new or updated information; but if they insist upon a full response then you would need to supply all the information.

6.5.4 The following examples are taken from the Information Commissioner's Office (ICO) Code of Practice for Subject Access Requests.

**Example**
A library receives a SAR from an individual who made a similar request one month earlier. The information relates to when the individual joined the library and the items borrowed. None of the information has changed since the previous request. With this in mind, along with the fact that the individual is unlikely to suffer any disadvantage if the library does not send any personal data in response, you need not comply with this request. However, it would be good practice to respond explaining why it has not provided the information again.

**Example**
A therapist who offers non-medical counselling receives a SAR from a client. She had responded to a similar request from the same client three weeks earlier. When considering whether the requests have been made at unreasonable intervals, the therapist should take into account the fact that the client has attended five sessions between requests, so there is a lot of new information in the file. She should respond to this request, and she could ask the client to agree that she only needs to send any 'new' information. But it would also be good practice to discuss with the client a different way of allowing the client access to the notes about the sessions.

If, for these reasons, you decide you are not obliged to provide the information requested, it is good practice to explain this to the requester. They may not realise, for example, that your records have not changed since their last request.

## 6.6 Manifestly unfounded or excessive requests?

6.6.1 You can ask for more information to help either identify the individual, or ask them to provide more information to enable a reasonable search to locate the information.

6.6.2 If the request is 'manifestly unfounded, excessive particularly because it is repetitive it is possible to charge a reasonable fee taking into account the administrative costs of providing the information or taking the action requested. Alternatively you can refuse to act on the request.

6.6.3 If you refuse the request you must inform the individual without undue delay and within one month of receipt of the request:

- the reasons you are not taking action;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through a judicial remedy.

## 6.7 CCTV Requests

6.7.1 The council has set a time-limit of 20 working days for responding to a request to access CCTV footage. Such requests are most likely to come from enforcement bodies and therefore not from the data subject. Such requests should be sent to ECSFeedback who will record and fulfil the request liaising with the CCTV Team. Were a data subject makes a request the timescale this should be responded to in line with the statutory timescales for responding to subject access requests.

## 7. PROCESSING A SUBJECT ACCESS REQUEST

7.1 The relevant FOI team will be assisted by the staff member (lead officer) within each department who has worked with or has knowledge of the individual concerned or information requested. Guidance and assistance will be provided by the FOI team to the lead officer at all stages of responding to the request.

7.2 If more than one department is required to fulfil a request, one of them must take the lead role. This will be agreed in negotiation between the departments. This must be decided before the letter of acknowledgement is sent to the applicant. If the request is transferred between departments it does not pause the running of the response time. Applicants should be encouraged to split large multi-departmental requests into a number of smaller separate requests. The applicant's original letter or form should be copied and sent to all relevant teams in each department and a single response time agreed or an agreement to respond individually (within the calendar month response time). Each department sends their data if it is sensitive.

7.3 The departmental FOI team can assist at any time and must be consulted if a request is to be refused due to a Data Protection Act exemption or any other reason. A reminder should be sent to the lead officer on day 15 by the relevant team and the applicant must be kept informed at all times, especially if it appears that the time limit will not be met. Lead officers must inform the relevant teams when the request has been fulfilled and provide the team with a copy of the response sent.

7.4 The DPA specifies that a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it would be reasonable for you to supply the information held when you send out a response, even if this is different to that held when the request was received. However, it is not acceptable to amend or delete the data if you would not otherwise have done so. For organisations subject to the Freedom of Information Act (FOIA), it is an offence to make such an amendment with the intention of preventing its disclosure.

### 7.5 Requests involving large amounts of information

7.5.1 Dealing with a subject access request (SAR) may be challenging. This might be because of the nature of the request, because of the amount of

personal data involved, or because of the way certain information is held. It may be useful to undertake an initial assessment of the size of the request and if need be discuss this with the requester.

7.5.2 You should be prepared to make extensive efforts to find and retrieve the requested information. Retain a record of the searches to locate the information as this will need to include a reference to this in your response.

7.5.3 Searches for information may include a search of email accounts. For the avoidance of doubt, the contents of an email should not be regarded as deleted merely because it has been moved to a user's 'Deleted items' folder.

7.5.4 It may be particularly difficult to find specific information contained in emails that have been archived and removed from 'live' systems. Nevertheless, the right of subject access is not limited to the personal data which it would be easy for you to provide, and the disproportionate effort exception cannot be used to justify a blanket refusal. It requires you to do whatever is proportionate in the circumstances. You may, of course, ask the requester to give you some context that would help you find what they want. Usually, once you have found the relevant emails, the cost of supplying a copy of the personal data within them is unlikely to be prohibitive.

## 7.6 Supplying information in permanent form – how the 'disproportionate effort' exception applies

7.6.1 The DPA requires us to provide a copy of the information in permanent form. There are two situations in which the obligation to supply the requester with a copy of the relevant information 'in permanent form' does not apply. The first is where the requester agrees to another arrangement, and the second is where the supply of such a copy is impossible or would involve disproportionate effort.

7.6.2 The 'disproportionate effort' exception is in section 95 of the DPA 2018, which is in part 3 of the Act, (Law Enforcement). Recital 93 of the GDPR allows us to ask the data subject, when a large quantity of data is involved, to specify the information or processing activities to which the request relates. In accordance with the DPA 1998 the Court of Appeal provided clarification as to its application in its 2017 judgments in the cases of Dawson–Damer[1] and Ittihadieh/Deer and Oxford University[2]. The DPA does not define 'disproportionate effort', but the court has explained that there is scope for assessing whether, in the circumstances of a particular case, complying with a request by supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's right of access to their personal data. The court also made it clear that, in assessing whether complying with a SAR would

[1] Dawson-Damer & Ors v Taylor Wessing LLP [2017] EWCA Civ 74
[2] Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd & Ors; Deer v University of Oxford and University of Oxford v Deer

involve disproportionate effort; the assessment should also take into account difficulties which occur throughout the process of complying with the request. This includes any difficulties encountered in finding the requested information.

7.6.3 When responding to SARs, the ICO expects us to evaluate the particular circumstances of each request, balancing any difficulties involved in complying with the request against the benefits the information might bring to the data subject, whilst bearing in mind the fundamental nature of the right of subject access.

7.6.4 In order to apply the exception, the burden of proof is on the council to show that all reasonable steps have been taken to comply with the SAR, and that it would be disproportionate in all the circumstances of the case for further steps to be taken.

7.6.5 It is good practice to engage with the requester, having an open conversation about the information they require. This might help to reduce the costs and the effort required to search for the information. Even if you can show that supplying a copy of information in permanent form would involve disproportionate effort, you must still try to comply with the request in some other way, if the applicant agrees. This could form a useful part of your discussions with the applicant, in order to identify an alternative way of satisfying their request.

## 7.7 Deciding what information to supply

7.7.1 Documents or files may contain a mixture of information that is the individual's personal data, personal data about other people and information that is not personal data at all. This means that sometimes you will need to consider each document within a file separately, and even the content of a particular document, to assess the information they contain.

7.7.2 It may be easier (and will be more helpful) to give a requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it is their personal data. This approach is likely to be appropriate where none of the information is particularly sensitive or contentious or refers to third-party individuals.

7.7.3 Subject access provides a right to see the information contained in personal data, rather than a right to see copies of the documents that include that information. You may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out of the relevant information from your computer systems. Although the easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so.

## 7.8 Requests involving other people's information

7.8.1 Responding to a SAR may involve providing information that relates to both the requester and another individual. The Act says you don't have to comply with a SAR if to do so would mean disclosing information about another identified individual except where:

- They have consented to the disclosure or
- It is reasonable in all the circumstances to comply with the request without their consent.

7.8.2 Third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual.

7.8.3 You need to consider the information on a case by case basis in order to make a decision. You need to balance the data subject's right of access against the other individual's rights. To help you decide the ICO suggests following a three-step process (see next page):

## Step 1 – does the request require disclosure of third party information?

Is it possible to comply with the request without revealing info to identify the third party?

You should take into account the information you are disclosing and any information you reasonably believe the person making the request may have, or may get hold of, that would identify the third-party individual.

As your obligation is to provide information rather than documents, you may delete names or edit documents if the third-party information does not form part of the requested information.

However, if it is impossible to separate the third-party information from that requested and still comply with the request, you need to take account of the following considerations.

## Step 2 – Has the third-party individual consented?

In practice, the clearest basis for justifying the disclosure of third party information in response to a SAR is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a SAR.

However, you are not obliged to try to get consent and in some circumstances it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. Indeed it may not always be appropriate to try to get consent, for instance if to do so would inevitably involve a disclosure of personal data about the requester
to the third party.

## Step 3 – Would it be reasonable in all the circumstances to disclose without consent?

In practice, it may sometimes be difficult to get third-party consent, e.g. the third party might refuse consent or might be difficult to find. If so, you must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway.

The DPA provides a non-exhaustive list of factors to be taken into account when making this decision. These include:

- any duty of confidentiality owed to the third-party individual;
- any steps you have taken to try to get the third-party individual's consent;
- whether the third-party individual is capable of giving consent; and
- any stated refusal of consent by the third-party individual.

If you have not got the consent of the third party and you are not satisfied that it would be reasonable in all the circumstances to disclose the third-party information, then you should withhold it. However, you are still obliged to communicate as much of the information requested as you can without disclosing the third-party individual's identity. Depending on the circumstances, it may be possible to provide some information, having edited or 'redacted' it to remove information that would identify the third-party individual.
You must be able to justify your decision to disclose or withhold information about a third party, so it is good practice to keep a record of what you decide, and why. For example, it would be sensible to note why you chose not to seek consent or why it was inappropriate to do so in the circumstances.

**Confidentiality**

7.8.4 Confidentiality is one of the factors that must be taken into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to the council with the expectation it will remain confidential. This expectation might result from the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and patient)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

7.8.5 However, you should not always assume confidentiality. For example, a duty of confidence does not arise merely because a letter is marked 'confidential' (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.

7.8.6 In most cases where a duty of confidence does exist, it will usually be reasonable to withhold third-party information unless you have the third-party individual's consent to disclose it.

7.8.7 Other factors will need to be taken into account:

- Information already known the individual and
- The individual's particular circumstances.

**Information generally known to the individual making the request**

7.8.8 If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely and reasonable to disclose that information. It is therefore helpful to have a conversation, wherever possible with the requester, when their request is first received.

**Circumstances relating to the individual making the request**

7.8.9 The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life.

Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent.

## 7.9 Editing information (Exemptions)

7.9.1 Some types of personal information are exempt from the right of subject access. Information may be exempt because of its nature or because the effect that its disclosure would have.

7.9.2 Where an exemption applies disclosure of some or all of the information may be refused depending on the circumstances. It is essential that a clear record is made of the decision making involved when processing a request. These will be required if the response is challenged to the ICO.

**Confidential references**

7.9.3 The Act contains an explicit exemption for confidential references, both given or received by the council if they are in respect to prospective or actual:

- education, training or employment of an individual
- placement of an individual as a volunteer or
- provision by an individual of any service.

7.9.4 The exemption applies to the right to be informed, that is, via a Privacy Notice and the right of access, via a Subject Access Request.

7.9.5 For example, we provide an employment reference in confidence for one of our employees to a company. If the employee makes a subject access request to the council or to the company, the reference will be exempt from disclosure. This is because the exemption applies to the reference regardless of whether it is in the hands of the employer that gives it or receives it.

**Publicly available information**

7.9.6 If an enactment requires the council to make information available to the public, any personal data included in it is exempt from the right of subject access.
The exemption only applies to the information that the organisation is required to publish.

**Crime and taxation**

7.9.7 Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:

- the prevention or detection of crime
- the capture or prosecution of offenders; and

- the assessment or collection of tax or duty.

7.9.8 If telling the individual that their data is being processed for one of these reasons would be likely to prejudice an investigation the exemption applies. A judgement needs to be taken in each case.

7.9.9 Schedule 2 3(2) of the DPA 2018 provides an additional exemption from the right of subject access that is designed to prevent the right being used to force relevant authorities to disclose information about the operation of crime detection and anti-fraud systems, where such disclosure may undermine the operation of those systems.

**Management information**

7.9.10 Personal data that is processed for management forecasting or management planning is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.

**Negotiations with the requester**

7.9.11 Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.

**Legal advice and proceedings**

7.9.12 Personal data is also exempt from the right of subject access if it consists of information for which legal professional privilege could be claimed in legal proceedings. This encompasses both 'legal advice' privilege and 'litigation' privilege. In broad terms, the former applies only to confidential communications between client and professional legal adviser, and the latter applies to confidential communications between client, professional legal adviser or a third party, but only where litigation is contemplated or in progress.

7.9.13 Where legal professional privilege cannot be claimed, you may not refuse to supply information in response to a SAR simply because the information is requested in connection with actual or potential legal proceedings. The DPA contains no exemption for such information; indeed, it says the right of subject access overrides any other legal rule that limits disclosure. In addition, there is
nothing in the Act that limits the purposes for which a SAR may be made, or which requires the requester to tell you what they want the information for.

**Social work records**

7.9.14 Special rules apply where providing subject access to information about social services and related activities would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health

or condition of the requester or any other person. These rules are set out in the Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI
2000/415). Their effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would be likely to cause such harm.

7.9.15 A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.

**Health, social work, education and child abuse records**

7.9.16 The exemptions that may apply when a SAR relates to personal data included in health, social work, education and child abuse records are explained in relevant section within the Information Commissioner's guide to exemptions.

**Other exemptions and further advice**

7.9.17 The Act contains additional exemptions that may be relevant when dealing with a SAR. More information about exemptions is now available from the ICO.

## 7.10 Redacting documents

7.10.1 Redaction is the term used to describe the preparation of information prior to disclosure. This includes obscuring permanently or temporarily information that must not be disclosed. Advice on this is provided within the council's Corporate Redaction Policy (intranet access required). In summary, the act of redaction can be done either:

- using the correct redaction software, such as Foxit Phantom (guidance can be obtained from ICT) or,
- by physically marking (obscuring) a hardcopy using opaque marker pen and then scanning it back in to create an electronic version

7.10.2 Care must be taken to ensure the redaction is adequate and that the information is neither visible nor retrievable. Using electronic markers, highlighting or adding black boxes to obscure information is not safe to use. You should not redact an original document, it should be copied and the copy redacted as above. Originals and redacted documents should also be clearly marked on files particularly when stored electronically within IT systems.

7.10.3 A copy of the original document must be retained for reference purposes and not disclosed unless specific approval has been obtained from your

manager. Further guidance can be sought from your departmental DIG representative

## 8. RESPONDING

8.1 The requester is entitled to a copy of the information in permanent form. It is important to consider the best way of securely sending this information to them particularly if there is a large amount of information. They may prefer to collect it from one of our offices or you may need to send via Special Delivery. It is important to verify the address that the response is sent to.

### 8.2 Explaining the information supplied

8.2.1 The GDPR requires that the information you provide to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child. At its most basic, this means that the additional information provided should be capable of being understood by the average person (or child). However, you are not required to ensure that that the information is provided in a form that can be understood by the particular individual making the request.

8.2.2 Any exemptions relied upon should be explained. The explanation should be provided in plain English and does more than simply stating the exemption.

### 8.3 What information needs to be included in the response?

8.3.1 Subject access entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- told whether any personal data is being processed – so, if you hold no personal data about the requester, you must still respond to let them know this;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- given details of the source of the data (if known).

8.3.2 This information might be contained in the copy of the personal data you supply. Where it is not included you need to supply this information in addition to a copy of the personal data itself when responding to a SAR. It is likely that this information is contained with a service privacy notice.

8.3.3 When responding to access to social care records it will be important to consider signposting to avenues of support may be needed. This is particularly important if the individual is or was in local authority care. Advice can be obtained from the CAH DIG representative.

8.3.4 The requester also needs to be advised as to their right of appeal should they remain dissatisfied with the response. In the first instance they should contact the lead officer or the relevant team to clarify any part of the response. Following this a review can be undertaken by a senior manager. The requester should also be told of their right to contact the Information Commissioner's Office at any time if they are not satisfied with their response, or the way their request has been handled, although they may ask the Council to resolve these concerns directly in the first instance.

## 8.4 Recording

8.4.1 It is important that a clear audit trail is retained showing the original documentation where the information disclosed was redacted due to reliance on an exemption. A SAR response audit should detail the decisions taken. This is available from your Departmental FOI Team.

8.4.2 A detailed record of the contents of subject access replies should be kept for 7 years in each department or stored in manual records. This record should include the information that was disclosed, and where necessary the exemptions that were used where information was not provided.

## 8.5 Reviewing

8.5.1 If a requester remains dissatisfied with the handling of their request they can request an internal review before approaching the ICO. As detailed in section 4.2 this should be carried out by a manager more senior than the lead officer who processed the original request.