Data protection

Subject access code of practice

Dealing with requests from individuals for personal information

ico.
Information Commissioner's Office

Contents

1 About this code of practice

Purpose of the code

This code of practice explains the rights of individuals to access their personal data. It also clarifies what you must do in this regard to comply with your duties as a data controller. These rights and duties are set out in sections 7–9A of the Data Protection Act 1998 (DPA) and are often referred to as 'the right of subject access', a phrase this code also uses. The code refers to a request made under section 7 of the DPA as a 'subject access request' (SAR).

The DPA's sixth data protection principle requires you to process personal data in accordance with the rights the Act gives to individuals. Subject access is one of those rights. The code is intended to help you provide subject access in accordance with the law and good practice. It aims to do this by explaining how to recognise a subject access request and by offering practical advice about how to deal with, and respond to, such a request. It provides guidance on the limited circumstances in which personal data is exempt from subject access. The code also explains how the right of subject access can be enforced when things go wrong.

Who should use the code of practice?

Any organisations that hold personal data should use the code to help them understand their obligations to provide subject access to that data, and to help them follow good practice when dealing with subject access requests. The good practice advice in the code will help all organisations – whether they are in the public, private or third sector. Although the practices that organisations adopt to respond to SARs are likely to differ, depending on their size and the nature of the personal data they hold, the underlying principles concerning subject access are the same in every case.

The code's status

The Information Commissioner has issued this code of practice under section 51 of the DPA as part of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the Act.

The code is the Information Commissioner's interpretation of what the DPA requires of organisations to comply with SARs. It gives advice on good practice, but compliance with our recommendations is not mandatory where they go beyond the strict requirements of

the DPA. The code itself does not have the force of law, as it is the DPA that places legally enforceable obligations on organisations.

Organisations may find alternative ways of meeting the DPA's requirements and of adopting good practice. However, if they do nothing they risk breaking the law. The ICO cannot take enforcement action over a failure to adopt good practice or to act on the code's recommendations unless this itself breaches the DPA.

We have tried to distinguish our good practice recommendations from the DPA's legal requirements. We provide advice about taking a positive approach to subject access in chapter 3 and, where appropriate, we list at the end of subsequent chapters some likely indicators that an organisation is dealing well with subject access. However, there is inevitably an overlap between the DPA's requirements and good practice: although the DPA sets out the legal requirements, it provides no guidance on the practical measures that could be taken to comply with them. This code helps to plug that gap.

More information

The code of practice is part of a series of guidance to help you as an organisation to fully understand your obligations under the DPA, as well as promoting good practice. You can find an overview of the DPA's main provisions in The ICO Guide to Data Protection.

The code is a guide to our general recommended approach, although decisions on individual cases will always be based on their particular circumstances.

If you need more information about this or any other aspect of data protection or freedom of information, please visit the ICO website: www.ico.org.uk

2 Overview of subject access

What is subject access?

Enabling individuals to find out what personal data you hold about them, why you hold it and who you disclose it to is fundamental to good information-handling practice. The Data Protection Act 1998 (DPA) gives individuals the right to require you to do this.

This right, commonly known as subject access, is set out in section 7 of the DPA. Individuals may exercise the right by making a written 'subject access request' (SAR).

What is personal data?

For information to be personal data, it must relate to a living individual and allow that individual to be identified from it (either on its own or along with other information likely to come into the organisation's possession). See chapter 5 for more guidance about the meaning of personal data.

Does a SAR have to be in a particular format?

No. A SAR simply needs to be made in writing and, if you require payment of a fee for dealing with the request, to be accompanied by the fee. You may not insist on the use of a particular form for making a SAR, but making a form available may assist the requester to provide the information you need to deal with their request.

How much is the fee?

Unless a SAR relates to one of a small number of special categories of information, the maximum fee you can charge for dealing with it is £10. Different fee limits apply where the request concerns health or educational records or credit files (explained in chapter 10 'Special cases').

What information is an individual entitled to?

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

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

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but you are not obliged to do this.

What is the time limit for responding?

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it.

Is any information exempt from subject access?

Yes. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also some restrictions on disclosing information in response to a SAR – where this would involve disclosing information about another individual, for example. Chapter 9 provides more detail on exemptions from subject access.

3 Taking a positive approach to subject access

Subject access is a fundamental right for individuals. But it is also an opportunity for you to improve your customer service and service delivery by responding to subject access requests (SARs) efficiently and transparently and by maximising the quality of the personal information you hold.

In our experience, most organisations want to help when an individual makes a SAR, whether that individual is their customer, an employee, or a stakeholder of some other kind. It makes good sense to help individuals exercise their information rights, rather than to hinder them. When things go wrong, complaints tend to follow. Many of the complaints we see could easily have been avoided by following the good practice advice in this code. In particular, if you clearly explain how individuals can request their personal information, what you need from them and what you will do in return – and if you keep to your word – you will probably avoid costly disputes and difficulties.

Adopting the good practice recommendations in this code will help you to:

- comply with your legal obligations under the Data Protection Act 1998 (DPA) – and show how you have done so;
- streamline your processes for dealing with SARs, saving you time and effort;
- increase levels of trust and confidence in your organisation by being open with individuals about the personal information you hold about them;
- retain your customers through better customer care;
- improve confidence in your information-handling practices;
- (if your organisation is in the public sector) improve the transparency of your activities in line with public policy requirements;
- enable customers, employees and others to verify that the information you hold about them is accurate, and to tell you if it is not; and
- improve your service delivery as a result.

An organisation that takes a positive approach to subject access might have the following indicators of good practice:

Training

All staff are trained to recognise a SAR as part of general data protection training. More detailed training on handling SARs is provided to relevant staff, dependent on job role.

Guidance

A dedicated data protection page is available for staff on the organisation's intranet with links to SAR policies and procedures.

Request handling staff

A specific person or central team is responsible for responding to requests. More than one member of staff is aware of how to process a SAR so there is resilience against absence.

In case requesters are dissatisfied with the initial response, arrangements are in place for a senior manager to review them.

Data protection experts

In a large organisation, there are data protection experts or 'information champions' to provide data protection expertise, including SAR advice, within departments where personal data is processed.

Monitoring compliance

Compliance with SARs is monitored and discussed at information governance steering group meetings, and management information is kept showing the number of SARs received. Details of any requests that have not been actioned within the statutory time limit are escalated to a suitably senior forum, so that any breach is tackled at a high level.

Additional indicators of good practice are given at the end of several subsequent chapters of the code. Not all of these indicators will be relevant to every organisation.

4 Recognising a subject access request

What is a subject access request?

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 request does not have to be in any particular form. Nor does it have to include the words 'subject access' or make any reference to the DPA. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act (FOIA).

Formal requirements

A SAR must be made in writing. Standard forms can make it easier for you to recognise a subject access request and make it easier for the individual to include all the details you might need to locate the information they want. However, there is no legally prescribed request form. Nor can you require individuals to use your own in-house form to make a SAR. You may invite individuals to use your own request form, but you should make clear that this is not compulsory and you must not try to use this as a way of extending the 40-day time limit for responding.

An emailed or faxed request is as valid as one sent in hard copy. SARs might also be received via social media (see below) and possibly via third-party websites. You may not insist on the use of a particular means of delivery for a SAR, but if you have a preference (eg by email to a particular mailbox) it is good practice to state clearly what it is. This should encourage requesters to submit SARs by the means you find most convenient, but you must still respond to SARs sent to you by other means.

You should also note the following points when considering validity.

- You do not need to respond to a request made orally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice at least to explain to the individual how to make a valid request, rather than ignoring them.
- If a request does not mention the DPA specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.

- Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with your organisation's SAR process.

Subject access requests and social media

Individuals may make a SAR using any Facebook page or Twitter account your organisation has, other social-media sites to which it subscribes, or possibly via third-party websites. This might not be the most effective way of delivering the request in a form you will be able to process quickly and easily, but there is nothing to prevent it in principle.

You should therefore assess the potential for SARs to be received via social-media channels and ensure that you take reasonable and proportionate steps to respond effectively to requests received in this way. However, as we explain in chapter 11, the Information Commissioner has discretion as to whether to take enforcement action and would not take it where it is clearly unreasonable.

You are entitled to satisfy yourself as to the identity of the person making the request. Because the requester must provide evidence of their identity and because you might require them to pay a fee, they will often have to supplement a SAR sent by social media with other forms of communication.

You may decline to use social media to supply information in response to a SAR if technological constraints make it impractical, or if information security considerations make it inappropriate to do so. In these circumstances you should ask for an alternative delivery address for the response.

Requests made on behalf of others

The 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, but it could simply be that an individual wants someone else to act for them. 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 to make the request or it might be a more general power of attorney.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather

than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

In some cases an individual does not have the mental capacity to manage their own affairs. There are no specific statutory provisions enabling a third party to exercise subject access rights on such a person's behalf. But it is reasonable to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority.

Requests for information about children

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 to anyone else, such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- where possible, 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 or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a SAR. The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases. It does not follow that, just because a child has capacity to make a SAR, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.

For more advice about data protection and children, see chapter 2 of our Personal information online code of practice.

There are separate rules about access to educational records – see chapter 10 'Special cases' for further guidance on this.

Dealing with freedom of information requests for the requester's personal data

As mentioned above, a valid SAR may, at first sight, appear to be something else. It is not uncommon, for example, for the request to state that it is a freedom of information (FOI) request. If, in reality, it relates to the requester's personal data, you must treat it as a subject access request.

Example

A local authority receives a letter from a council tax payer requesting a copy of any information the authority holds about a dispute over his eligibility for a discount. The letter states it is a 'freedom of information request'. It is clear that the request concerns the individual's own personal data and the local authority should treat it as a subject access request.

You may be more likely to receive a SAR in the form of a freedom of information request if your organisation is a public authority for the purposes of FOIA or the Environmental Information Regulations 2004 (EIR). Whether or not the organisation is a public authority, however, you must deal with the request appropriately, and this will depend on whether it relates only to the requester's own personal data or to other information as well.

If it is clear that the requester is merely asking for their own personal data, but they have cited FOIA, you should do the following:

- Deal with the request as a SAR in the normal way. The requester does not need to make a new request. You may need to ask for payment of any necessary fee or ask the individual to verify their identity.
- If your organisation is a public authority, the requested personal data is, in fact, exempt from disclosure under FOIA or the EIR. Strictly speaking, you should issue a formal refusal notice saying so. In practice, however, we would not expect you to do this if you are dealing with the request as a SAR.
- It is good practice for public authorities to clarify within 20 working days (the time limit for responding to FOI requests) that the request is being dealt with as a SAR under the DPA, and that the 40-day time limit for responding applies.

If the request relates to information that cannot be requested by means of a SAR (eg it includes a request for non-personal information) then, if your organisation is a public authority, you should treat this as two requests: one for the requester's personal data made under the DPA; and another for the remaining, non-personal information made under FOIA. If any of the non-personal information is environmental, you should consider this as a request made under the EIR.

It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA or the EIR is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA or the EIR to the world at large, this could lead to a breach of the data protection principles.

For more information on dealing with FOI requests, please see the Guide to FOIA.

For more information on the exemption from FOIA for personal data, please see ICO guidance:

- Section 40: personal information
- Section 40: applying the exemption for third party personal data
- Section 40: access to information held in complaint files
- Section 40: requests for personal data about public authority employees

For more about dealing with requests for environmental information, please see the Guide to EIR.

An organisation that is alert to the need to deal with SARs effectively might have the following indicators of good practice:

Guidance

Guidance on making a SAR, along with a form, is made available on the organisation's website. The guidance:

- makes it clear where the request should be sent to;
- highlights the fee and explains the options for payment;
- specifies the information that the requester will need to provide to confirm their identity;
- mentions the 40-day period for responding to the request; and
- gives details of a point of contact for any questions.

While using a form is not mandatory, when it is used it helps to identify SARs. The form includes a 'for office use only' type section providing instructions to the receiver on what to do with the form, and space to record certain information to assist in processing the request (such as the date the form was received, whether ID has been checked and whether a fee has been paid).

Guidance has been produced for staff to help them identify SARs. In particular, this has been directed at those members of staff who deal with personal data, such as staff in human resources. The guidance, which is available on the organisation's intranet, explains what staff should do if they receive a SAR and stresses the need to act promptly and refer it to the right team.

Training

Data protection training includes a section on SARs and dealing with subject access. It also teaches staff about their own rights as data subjects (to put the training in context). There is a test at the end with a pass mark, and attendance is included as a performance objective for some staff.

Staff dealing with incoming correspondence, for example in the mailroom, are trained in how to recognise a SAR and to ensure that requests are delivered promptly to the relevant people.

If the organisation operates a shift-working system, the training is repeated at times that ensure all staff have the opportunity to attend.

5 Responding to a subject access request – general considerations

Subject access is a right of access to the personal data of a particular individual

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Before you can respond to a subject access request (SAR), you need to be able to decide whether information you hold is personal data and, if so, whose personal data it is.

The Data Protection Act 1998 (DPA) provides that, for information to be personal data, it must relate to a living individual and allow that individual to be identified from that information (either on its own or in conjunction with other information likely to come into the organisation's possession). The context in which information is held, and the way it is used, can have a bearing on whether it relates to an individual and therefore on whether it is the individual's personal data.

In most cases, it will be obvious whether the information being requested is personal data, but we have produced separate guidance (Determining what is personal data) to help you decide in cases where it is unclear.

The same information may be the personal data of two (or more) individuals. Additional rules apply where responding to a SAR may involve providing information that relates both to the individual making the request and to another individual. These rules are explained in chapter 7.

Responsibility of the data controller

If you determine the purpose for which and the manner in which the personal data in question is processed, then you (or your organisation) are/is the data controller in relation to that personal data and will be responsible for responding to the SAR. The DPA does not allow any extension to the 40-day time limit where you have to rely on a data processor to provide the information you need to respond.

Example

An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party data processor is analysing the information.

The employer receives a SAR from a member of staff. To respond, the employer needs information held by the data processor. The employer is the data controller for this information and should instruct the data processor to retrieve any personal data that relates to the member of staff.

If you use a data processor, you need to make sure you have contractual arrangements in place to guarantee that SARs are dealt with properly, irrespective of whether they are sent to you or to the data processor.

The role of a data processor is explained in the ICO Guide to Data Protection.

Information management systems

You will find it difficult to deal with SARs effectively without adequate information management systems and procedures. Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs. Not only should your systems have the technical capability to search for the information necessary to respond to a SAR, but they should also operate by reference to effective records management policies. For example, it is good practice to have a well-structured fileplan and standard file-naming conventions for electronic documents, and for the retention and deletion of documents to be governed by a clear retention policy. If you are buying a new information management system, you should consider including requirements in the specification about searching and SARs.

Time limits

You must comply with a SAR 'promptly' and in any event within 40 days of the date on which the request is received or (if later) the day on which you receive:

- the fee (if any);
- any requested location information (see chapter 6); and
- any information requested to confirm the requester's identity (see below for further guidance).

The duty to comply promptly with a SAR clearly implies an obligation to act without unreasonable delay but, equally clearly, it does not oblige you to prioritise compliance over everything else. The 40-day long-stop period is generally accepted as striking the right balance in most cases between the rights of individuals to prompt access to their personal data and the need to accommodate the resource constraints of organisations to which SARs are made. Provided that you deal with the request in your normal course of business, without unreasonable delay, and within the 40-day period, you are likely to comply with the duty to comply promptly.

Fees and cost limits

You may charge a fee for dealing with a SAR. If you choose to do this, you need not comply with the request until you have received the fee. The maximum fee you can charge is normally £10 (including any card-handling or administration charges). There are different fee structures for organisations that hold health or education records (where the maximum fee is £50, depending on the circumstances – see chapter 10). These fees are not subject to VAT.

You need not comply with a request until you have received the fee, but you cannot ignore a request simply because the individual has not sent a fee. If a fee is payable but has not been sent with the request, you should contact the individual promptly and inform them that they need to pay.

Some organisations choose not to charge a fee. However, once you have started dealing with an individual's request without asking for a fee, it would be unfair to then demand a fee as a way of extending the period of time you have to respond to the request.

In many cases the fee you may charge for dealing with a SAR will not cover the administrative costs of doing so. You must comply with the request regardless of this fact.

There is one narrowly defined situation in which the likely cost of complying with a SAR is relevant in determining whether an organisation must comply. Where a request relates to 'unstructured personal data' (as defined in section 9A(1) of the DPA) held by a public authority, the authority is not required to comply with the request if it estimates that the cost of doing so would exceed either £450 or £600. The relevant limit depends on the identity of the public authority (see the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004).

Making reasonable adjustments for disabled people

Some disabled people find it difficult to communicate in writing, and may therefore have difficulty making a SAR. You may have a legal duty to make reasonable adjustments for such a person if they wish to make a SAR. Reasonable adjustments could include treating a verbal request for information as though it were a valid SAR. If the request is complex, it would be good practice for you to document it in an accessible format and to send it to the disabled person to confirm the details of the request.

You might also have to respond in a particular format that is accessible to the disabled person, such as Braille, large print, email or audio formats. If an individual thinks you have failed to make a reasonable adjustment, they may make a claim under the applicable equality legislation. Information about making a claim is available from the Equality and Human Rights Commission or from the Equality Commission for Northern Ireland.

Confirming the requester's identity

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that you know the identity of the requester. You can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on their behalf).

The key point is that you must be reasonable about what you ask for. You should not request a lot more information if the identity of the person making the request is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

Example

You have received a written SAR from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your organisation's policy is to verify identity by asking for a copy of a utility bill, it would be unreasonable to do so in this case since you know the person making the request.

However, you should not assume that, on every occasion, the person making a request is who they say they are. In some cases, it is reasonable to ask the person making the request to verify their identity before sending them information.

Example

An online retailer receives a SAR by email from a customer. The customer has not used the site for some time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, before responding to the request it would be reasonable to gather further information, which could be as simple as asking the customer to confirm other account details such as a customer reference number.

The means by which the SAR is delivered might affect your decision about whether you need to confirm the requester's identity. For example, if a request is made by means of an email account through which you have recently corresponded with the requester, you may feel it is safe to assume that the SAR has been made by the requester. On the other hand, if the request is made via a social networking website, it would be prudent to check it is a genuine request.

The level of checks you should make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.

Example

A GP practice receives a SAR from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requester is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for more information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious. They could ask the requester to provide more information, such as a document providing evidence of date of birth or passport.

Before supplying any information in response to a SAR, you should also check that you have the requester's correct postal or email address (or both). If you are supplying information by fax (and we recommend that you do so only if the requester specifically asks you to), then you must ensure that you are sending it to the correct fax number.

Where a requester dies before the response is provided

As stated earlier, the definition of personal data covers "data which relate to a living individual". If a requester dies before a response is provided but the data controller received the SAR when the individual was living, it must provide the response to the individual's personal representatives. As a matter of good customer service we suggest that it would be advisable for data controllers who are aware that the data subject has died and who know the identity of the personal representative(s) to check with them if they in fact still wish to receive the information, before sending it.

Dealing with bulk requests

Depending on the size of your organisation and the nature of your business, you may from time to time receive several (and possibly many) SARs in a short period of time. In the financial services sector, for example, it is not uncommon for 'bulk' requests to be made by claims management companies on behalf of multiple individuals.

Each SAR within a bulk request must be considered individually and responded to appropriately. The Information Commissioner acknowledges the potential resource implications of this duty but recommends you bear in mind the following principles when dealing with high volumes of SARs:

- a SAR that is made as part of a bulk request has the same legal status as a SAR that is made individually;
- the purpose for which a SAR is made does not affect its validity, or your duty to respond to it;
- if the request is made by a third party on behalf of the individual concerned, you are entitled to satisfy yourself that the third party is authorised to make the request;
- you are also entitled to satisfy yourself as to the identity of the individual concerned;
- you must respond to the request even if you hold no information about the individual. Your response may obviously be very brief in such cases; and
- you should be prepared to respond to peaks in the volume of SARs you receive.

In considering a complaint about a SAR, the ICO will have regard to the volume of requests received by an organisation and the steps it has taken to ensure requests are dealt with appropriately even in the face of a high volume of similar requests. The organisation's size and resources are likely to be relevant factors. As we explain in chapter 11, the Information Commissioner has discretion as to whether to take enforcement action and would not take such action where it is clearly unreasonable to do so.

An organisation that responds effectively to SARs might have the following indicators of good practice:

Managing expectations

Guidance on the organisation's website mentions the 40-day time limit for responding to a SAR and each request is acknowledged with a letter or email informing the requester of the date by which a response must be provided. If there is a delay in dealing with the request for any reason, the organisation contacts the requester to explain the reason and the expected date for the response.

The response to a SAR includes an explanation of the searches that have been made to deal with the request and the information revealed by those searches. This helps the requester understand whether they have received all the information they are entitled to.

Logs and checklists

The organisation logs receipt of SARs and updates it to monitor progress as the SAR is processed. The log includes copies of information supplied in response to the SAR, together with copies of any material withheld and an explanation why.

A standard checklist is used to ensure consistency in identity verification procedures and fee collection, and to ensure that the necessary information is obtained from relevant departments across the organisation. The checklist forms a cover-sheet on the file for each SAR received.

Systems, technology and contracts

Reliable indexes, file contents pages, descriptions of documents and metadata make it easier for those dealing with SARs to locate personal data, decide whose personal data it is and make decisions about its disclosure.

In a larger organisation, a dedicated IT system is used to process SARs. This enables the organisation effectively to manage and monitor requests received. The system records all correspondence, identity confirmation enquiries and fee payments. In addition it records details of the request, such as date received and date when response is due, and generates reports to monitor compliance.

Where a data processor is involved, the organisation ensures the data processor is aware of its obligations with regard to subject access before appointment. A clause specifying the organisation's requirements for SAR handling is included in the written contract.

6 Finding and retrieving the relevant information

Extent of the duty to provide subject access

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. In this chapter we consider the extent of the right of subject access in relation to categories of information that may be difficult to access. We also explain what additional information you may require from the requester to help you find the data they want.

The DPA does not permit you to exclude information from your response to a SAR merely because it is difficult to access. The Act deals with the situation where supplying information in permanent form to the requester is impossible or would involve disproportionate effort (see chapter 8). But it does not place any express limits on your duty to search for and retrieve the information they want.

You should be prepared to make extensive efforts to find and retrieve the requested information. Even so, you are not required to do things that would be unreasonable or disproportionate to the importance of providing subject access to the information. Any decision on these matters should reflect the fact that the right of subject access is fundamental to data protection. It will always be reasonable and proportionate to search your records in the manner recommended in this chapter, and to review the information found with a view to disclosing it; and it will never be reasonable to deny access to the requested information merely because responding to the request may be labour-intensive or inconvenient.

Clarifying the request

Before responding to a SAR, you may ask the requester for information you reasonably need to find the personal data covered by the request. You need not comply with the SAR until you have received it. However, even if the relevant information is difficult to find and retrieve, it is not acceptable for you to delay responding to a SAR unless you reasonably require more information to help you find the data in question.

Example

A chain of supermarkets is dealing with a general SAR from a member of staff at one of its branches. The person dealing with the request is satisfied that the staff member has been sent all information held in personnel files and in files held by his line manager. However, he complains that not all information about him was included in the response.

The employer should not ignore this complaint, but it would be reasonable to ask him for more details. For example, some of the information may be in emails, and the employer could reasonably ask for the approximate dates when the emails were sent and who sent them, to help find what he wants.

It might also be useful for the employer to ask if the member of staff is seeking information that does not relate to his employment. For example, he may be seeking information that relates to a complaint he made as a customer of the supermarket.

You cannot require the requester to narrow the scope of their request, but merely to provide additional details that will help you locate the requested information. So, if a requester asks for 'all the information you hold' about them, they are entitled to do that. You may ask them to provide information about the context in which information about them may have been processed, and about the likely dates when processing occurred, if this will help you deal with the request.

As with a request that is sent without the required fee, you should not ignore a request simply because you need more information from the requester. You should not delay in asking for this, but should ensure the requester knows you need more information and should tell them what details you need. Provided you have done that, the 40-day period for responding to the request does not begin to run until you have received the appropriate fee and any additional information you need.

The type of information it might be reasonable for you to ask for includes, where personal data is held in electronic form, information as to the type of electronic data being sought (application form, letter, email etc) and roughly when the data was created. This may help you identify whether the information sought is likely to have been deleted or archived (either printed off and held in a manual data archive, or removed from your 'live' electronic data systems and held in an electronic archive).

Electronic records

In most cases, information stored in electronic form can easily be found and retrieved. However, as it is very difficult to truly erase all electronic records, it is arguable that a requester might be entitled to request access to personal data that you do not have ready access to – because you still hold the data and, with time and varying degrees of technical expertise, you could retrieve it.

You are likely to have removed information from your 'live' systems in a number of different ways. The information may have been:

- 'archived' to storage;
- copied to back-up files; or
- 'deleted'.

Archived information and back-up records

Generally speaking, information is archived because, although you wish to remove it from your live systems, you decide to retain a copy in case it is needed in the future.

You should have procedures in place to find and retrieve personal data that has been electronically archived or backed up. The process of accessing electronically archived or backed-up data may be more complicated than the process of accessing 'live' data. However, as you have decided to retain copies of the data for future reference, you will presumably be able to find the data, possibly with the aid of location information from the requester. So you will be required to provide such information in response to a SAR.

Electronic archive and back-up systems might not use such sophisticated search mechanisms as 'live' systems, and you may ask a requester to give you enough context about their request to enable you to make a targeted search. The requester's ability to provide it may significantly affect whether you can find what they want. Nevertheless, to the extent that your search mechanisms allow you to find archived or backed-up data for your own purposes, you should use the same effort to find information in order to respond to a SAR.

If a request relates specifically to back-up copies of information held on your 'live' systems, it is reasonable to consider whether there is any evidence that the back-up data differs materially from that which is held on the 'live' systems and which has been supplied to the requester. If there is no evidence that there is any material difference, the Information Commissioner would not seek to enforce the right of subject access in relation to the back-up records.

Deleted information

Information is 'deleted' when you try to permanently discard it and you have no intention of ever trying to access it again. The Information Commissioner's view is that, if you delete personal data held in electronic form by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean you must go to such efforts to respond to a SAR. The Commissioner would not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form. The Commissioner does not require organisations to expend time and effort reconstituting information that they have deleted as part of their general records management.

In coming to this view, the Information Commissioner has considered that the purpose of subject access is to enable individuals to find out what information is held about them, to check its accuracy and ensure it is up to date and, where information is incorrect, to request correction of the information or compensation if inaccuracies have caused them damage or distress. However, if you have deleted the information, you can no longer use it to make decisions affecting the individual. So any inaccuracies can have no effect as the information will no longer be accessed by you or anyone else.

For more information on deleted information, please see the ICO guidance on Deleting personal data.

Information contained in emails

The contents of emails stored on your computer systems are, of course, a form of electronic record to which the general principles above apply. 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.

It may be particularly difficult to find information to which a SAR relates if it is contained in emails that have been archived and removed from your 'live' systems. Nevertheless, the right of subject access is not limited to the personal data to which it would be easy for you to provide access. Subject to certain exemptions, you must provide subject access to all personal data you hold, even if it is difficult to find. 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. You cannot refuse to comply with a SAR on the basis that it would involve disproportionate effort, simply because it would be costly and time consuming to find the requested personal data held in archived emails.

Information stored on personal computer equipment

You are only obliged to provide personal data in response to a SAR if you are a data controller in respect of that data. In most cases, therefore, you do not have to supply personal data if it is stored on someone else's computer systems rather than your own (the obvious exception being where that person is a data processor (see chapter 5)). However, if the requester's personal data is stored on equipment belonging to your staff (such as smartphones or home computers) or in private email accounts, what is the position when you receive a SAR?

It is good practice to have a policy restricting the circumstances in which staff may hold information about customers, contacts, or other employees on their own devices or in private email accounts. Some organisations enable staff to access their systems remotely (eg via a secure website), but most are likely to prohibit the holding of personal data on equipment the organisation does not control. Nevertheless, if you do permit staff to hold personal data on their own devices, they may be processing that data on your behalf, in which case it would be within the scope of a SAR you receive. The purpose for which the information is held, and its context, is likely to be relevant in this regard. We would not expect you to instruct staff to search their private emails or personal devices in response to a SAR unless you have a good reason to believe they are holding relevant personal data.

For more advice about what you need to consider when permitting the use of personal devices to process personal data for which you are responsible, see our Bring your own device (BYOD) guidance.

As we explain in chapter 11, the Commissioner has discretion as to whether to take enforcement action where there has been a breach of the DPA. The Information Commissioner would not take such action where it is clearly unreasonable to do so.

Other records

If you hold information about the requester otherwise than in electronic form (eg in paper files or on microfiche records), you will need to decide whether it is covered by the right of subject access. You will need to make a similar decision if electronic records have been removed from your live systems and archived in non-electronic form.

Whether the information in such hard-copy records is personal data accessible via the right of subject access will depend primarily on whether the non-electronic records are held in a 'relevant filing system' and also on whether the requester has given you enough context to enable you to find it.

For further guidance on relevant filing systems, see The Guide to Data Protection and the guidance FAQs about relevant filing systems on our website. Broadly speaking, however, we consider that a

relevant filing system exists where information about individuals is held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.

Amending data following receipt of a SAR

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 you hold when you send out a response, even if this is different to that held when you received the request.

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.

An organisation that is effective in finding and retrieving the information it needs to respond to a SAR might have the following indicators of good practice:

Seeking clarification

There is an optional standard form for making a SAR. The form invites the requester to give details of the specific information requested. Often, by narrowing the scope of the request (where feasible) you can avoid making unnecessary searches or sending the requester large amounts of information they do not want or expect.

As part of the SAR logging process, the clarity of the request is checked. If it is not immediately obvious what the request relates to or where the required personal information is located, the organisation contacts the requester by phone to seek clarification.

A check is also made to ensure that the organisation knows the address where it will send the response.

Asset registers

An information asset register is in place that states where and how personal data is stored. This helps speed up the process of locating the information required to respond to SARs. Information asset owners are in place and the register is regularly reviewed to ensure it is kept up to date.

Retention and deletion policies

There are documented retention and deletion policies relating to the personal information the organisation holds. Different retention periods apply to different classes of information, depending on the purpose for which it is held.

Monitoring

If the organisation receives a significant volume of SARs, appropriate governance structures are in place to ensure they are processed and responded to effectively. For example, the team responsible for dealing with SARs holds weekly meetings to discuss SARs' progress and to investigate any cases that appear to be facing delay.

7 Dealing with subject access requests involving other people's information

The basic rule

Responding to a subject access request (SAR) may involve providing information that relates both to the requester and another individual.

Example

An employee makes a request to her employer for a copy of her human resources file. The file contains information identifying managers and colleagues who have contributed to (or are discussed in) that file. This will require you to reconcile the requesting employee's right of access with the third parties' rights in respect of their own personal data.

The Data Protection Act 1998 (DPA) says you do not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

You should make decisions about disclosing third-party information on a case-by-case basis. You must not apply a blanket policy of withholding it.

For the avoidance of doubt, you cannot refuse to provide subject access to personal data about an individual simply because you obtained that data from a third party. The rules about third-party information, described in this chapter, apply only to personal data

that includes information about the individual who is the subject of the request and information about someone else.

Three-step approach to dealing with information about third parties

To help you decide whether to disclose information relating to a third-party individual, it helps to follow the three-step process described below. The ICO guidance Access to information held in complaint files also gives more advice about this.

Step 1 – Does the request require the disclosure of information that identifies a third party?

You should consider whether it is possible to comply with the request without revealing information that relates to and identifies a third-party individual. In doing so, 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.

Example

In the previous example about a request for an employee's human resources file, even if a particular manager is only referred to by their job title it is likely they will still be identifiable based on information already known to the employee making the request.

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, eg 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.

Confidentiality

Confidentiality is one of the factors you must take 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 you 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)

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.

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.

Other relevant factors

In addition to the factors listed in the DPA, the following points are likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

- **Information generally known by the individual making the request.** 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 to be reasonable for you to disclose that information. It follows that 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.
- **Circumstances relating to the individual making the request.** 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.
- **Health, educational and social work records.** As explained in chapters 9 and 10, special rules govern subject access to health, educational and social-work records. In practice, these rules mean that relevant information about health, education or social work professionals (acting in their professional capacities) should usually be disclosed in response to a SAR.

Responding to the request

Whether you decide to disclose information about a third party in response to a SAR or to withhold it, you will need to respond to the requester. If the third party has given their consent to disclosure of information about them or if you are satisfied that it is reasonable in all the circumstances to disclose it without consent, you should provide the information in the same way as any other information provided in response to the SAR.

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.

8 Supplying information to the requester

Information that must be supplied

The focus of a subject access request (SAR) is usually the supply of a copy of the requester's personal data. In this chapter we consider a number of issues about supplying that information. However, you should remember that 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).

This information might be contained in the copy of the personal data you supply. To the extent it is not, however, you must remember to supply this information in addition to a copy of the personal data itself when responding to a SAR.

The right to a description of other organisations or people to whom personal information may be given is a right to this information in general terms; it is not a right to receive the names of those organisations or people.

The requester may also ask for an explanation of the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret). You only need to provide this additional information if it has been specifically requested.

Before supplying any information in response to a SAR, you should check that you have the requester's correct postal or email address (or both). If you are supplying information by fax (and we recommend that you do so only if the requester specifically asks you to), then you must ensure you are sending it to the correct fax number.

Deciding what information to supply

Documents or files may contain a mixture of information that is the requester'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.

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.

Form in which the information must be supplied

Once you have located and retrieved the personal data that is relevant to the request, you must communicate it to the requester in intelligible form. In most cases, this information must be communicated to the requester by supplying him or her with a copy of it in permanent form. You may comply with this requirement by supplying a photocopy or print-out of the relevant information.

But if the requester has made a SAR electronically, they will probably be content – and may even prefer – to receive the response electronically too. It is good practice to check their preference. If they agree to receive information in electronic form, you will comply with the DPA by sending it in that form.

Some requesters are starting to ask for certain personal data (such as their domestic energy consumption data) to be supplied to them in an 'open re-usable format', for example a CSV file. Offering the data in this format makes it far easier for the data to be used by the requester under their control in relation to other services. The Information Commissioner would encourage you to consider the feasibility of enabling requesters to receive their data in open re-usable formats, for appropriate datasets. Clearly, we recognise that the cost and practicality of doing so must be taken into account. Such an approach is consistent with the Government's 'Midata' project, which aims to allow people to view, access and use their personal and transaction data in a way that is portable and safe.

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.

Explaining the information supplied

The DPA requires that the information you supply to the individual is in intelligible form. At its most basic, this means the information should be understandable by the average person. However, the DPA does not require you to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

Example

An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as 'A', while non-attendance at a similar event is logged as 'M'. Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to the organisation's key or index to explain this information, it would be impossible for anyone outside the organisation to understand. In this case, the Act requires you to explain the meaning of the coded information. However, although it would be good practice to do so, the Act does not require you to decipher the poorly written notes, since the meaning of 'intelligible form' does not extend to 'make legible'.

Example

You receive a SAR from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. The Act does not require you to do this since the information is in intelligible form, even if the person who receives it cannot understand all of it. However, it would be good practice for you to help them understand the information you hold about them.

Example

Your organisation is based in Wales and your language of business is Welsh, not English, which means the documents you hold are all in Welsh. You receive a SAR from someone who does not speak or understand Welsh. After receiving your response, they ask you to translate the information. The Act does not require you to do this since the information is in intelligible form, even if the person cannot understand it. However, it would be good practice for you to help them understand the information you hold about them. Of course there may also be a separate requirement for you to translate the information under Welsh-language legislation, but this falls outside the scope of the DPA.

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

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. The so-called 'disproportionate effort' exception is in section 8(2) of the DPA. It has caused considerable confusion.

The DPA does not define 'disproportionate effort' but it is clear that there is some (albeit limited) scope for assessing whether 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.

We stress that you should rely on the disproportionate effort exception only in the most exceptional of cases. The right of subject access is central to data protection law and we rarely hear of instances where an organisation could legitimately use disproportionate effort as a reason for denying an individual access to any of their personal data. Even if you can show that supplying a copy of information in permanent form would involve disproportionate effort, you must still comply with the request in some other way.

Example

An organisation has decided that to supply copies of an individual's records in permanent form would involve disproportionate effort. Rather than refuse the individual access, they speak to her and agree that it would be preferable if she visited their premises and viewed the original documents. They also agree that if there are documents she would like to take away with her, they can arrange to provide copies.

In addition, even if you do not have to supply a copy of the information in permanent form, the requester still has the right:

- to be informed whether you are processing their personal data; and
- if so, to be given a description of:
  - the personal data in question;
  - the purpose of the processing; and
  - the recipients or classes of recipients; and
- to be given information about the source of the personal data.

Dealing with repeated or unreasonable requests

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.

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.

Section 8(6) of the DPA states that the "information to be supplied pursuant to a request… must be supplied by reference to the data in question at the time when the request is received… ". 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.

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.

An organisation that has effective mechanisms in place for supplying information to requesters might have the following indicators of good practice.

Online and electronic formats

Where appropriate, customers are able to access their personal information free of charge by using a secure website. This is good customer service and is likely to reduce the number of SARs the organisation has to deal with.

If requested, personal information is supplied in a machine-readable and re-usable format.

Onsite viewing facilities

There are procedures in place for requesters to view the requested information on the premises if it is voluminous or may require further support or explanation or both.

Copy differentiation

SAR-response hard copies are stamped 'data subject copy' before release. This may help identify the source of any further disclosure of the information, should the need arise.

9 Exemptions

Exemptions and restrictions – general

The Data Protection Act 1998 (DPA) recognises that in some circumstances you might have a legitimate reason for not complying with a subject access request (SAR), so it provides a number of exemptions from the duty to do so. Where an exemption applies to the facts of a particular request, you may refuse to provide all or some of the information requested, depending on the circumstances. It is a matter for you to decide whether or not to use an exemption – the DPA does not oblige you to do so, so you are free to comply with a SAR even if you could use an exemption.

Certain restrictions (similar to exemptions) are also built into the DPA's subject access provisions. For example, there are restrictions on the disclosure of personal data about more than one individual in response to a SAR (see chapter 7).

This chapter of the code explains the operation of the main exemptions from the duty to provide subject access. Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies in a particular SAR. Some exemptions apply because of the nature of the personal data in question, eg information contained in a confidential reference. Others apply because disclosure of the information would be likely to prejudice a particular function of the organisation to which the request is made. The DPA does not explain what is meant by 'likely to prejudice'. However, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned.

If challenged, you must be prepared to defend to the Information Commissioner's Office or a court your decision to apply an exemption. It is therefore good practice to ensure that such a decision is taken at a suitably senior level in your organisation and that you document the reasons for it.

Confidential references

From time to time you may give or receive references about an individual, eg in connection with their employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access.

The DPA distinguishes between references you give and references you receive.

References you give are exempt from subject access if you give them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.

There is no such exemption for references you receive from a third party. If you receive a SAR relating to such a reference, you must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

Example

Company A provides an employment reference for one of its employees to company B. If the employee makes a SAR to company A, the reference will be exempt from disclosure. If the employee makes the request to company B, the reference is not automatically exempt from disclosure and the usual subject access rules apply.

It may be difficult to disclose the whole of a reference to the individual it relates to without disclosing some personal data about the author of the reference – most obviously, their identity. If the reference was not provided in confidence, this difficulty should not prevent disclosure. However, if a question of confidentiality arises, you should contact the author to find out whether they object to the reference being disclosed and, if so, why.

Even if the provider of a reference objects to its disclosure in response to a SAR, you will need to supply the personal data it contains to the requester if it is reasonable to do so in all the circumstances. You will therefore need to weigh the referee's interest in having their comments treated confidentially against the requester's interest in seeing what has been said about them. Relevant considerations are likely to include:

- any clearly stated assurance of confidentiality given to the referee;
- any reasons the referee gives for withholding consent;
- the likely impact of the reference on the requester;
- the requester's interest in being able to satisfy himself or herself that the reference is truthful and accurate; and
- any risk that disclosure may pose to the referee.

For more advice about how to deal with SARs that include personal data about third parties, see chapter 7.

Publicly available information

If an enactment requires an organisation 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. If it holds additional personal data about an individual, the additional data is not exempt from the right of subject access even if the organisation publishes it.

Crime and taxation

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.

Example

The police process an individual's personal data because they suspect him of involvement in a serious crime. If telling the individual they are processing his personal data for this purpose would be likely to prejudice the investigation (perhaps because he might abscond or destroy evidence), then the police do not need to do so.

However, the exemption applies, in any particular case, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above. You need to judge whether or not this is likely in each case – you should not use the exemption to justify denying subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

Example

A taxpayer makes a SAR to Her Majesty's Revenue and Customs (HMRC) for personal data they hold about him in relation to an ongoing investigation into possible tax evasion. If disclosing the information which HMRC have collected about the taxpayer would be likely to prejudice their investigation, eg because it would make it difficult for them to collect evidence, HMRC could refuse to grant subject access to the extent that doing so would be likely to prejudice their investigation.

If, however, the taxpayer does not make the request until some years later when the investigation (and any subsequent prosecution) has been completed, it is unlikely that complying with the SAR would prejudice the crime and taxation purposes – in which case HMRC would need to comply with it.

Nor would the exemption justify withholding all the personal data to which the request relates when only part of the personal data would be likely to prejudice those purposes.

Example

In the previous example about an ongoing investigation into possible tax evasion, HMRC would be entitled to refuse subject access to personal data that would be likely to prejudice their investigation. However, this would not justify a refusal to grant access to other personal data they hold about the taxpayer.

Personal data that:

- is processed for the purpose of discharging statutory functions; and
- consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above

is also exempt from the right of subject access to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the right applying to personal data that is passed to statutory review bodies by law-enforcement agencies, and ensures that the exemption is not lost when the information is disclosed during a review.

Example

The Independent Police Complaints Commission (IPCC) begins an investigation into the conduct of a particular police force. Documents passed to the IPCC for the purposes of the investigation contain personal data about Mr A that the police force would not have been obliged to disclose to Mr A in response to a SAR – because doing so would be likely to prejudice its criminal investigation. If Mr A then makes a SAR to the IPCC, he has no greater right of access to the personal data in question.

Section 29(4) of the DPA 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

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data 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.

Example

The senior management of an organisation are planning a re-organisation. This is likely to involve making certain employees redundant, and this possibility is included in management plans. Before the plans are revealed to the workforce, an employee makes a SAR. In responding to that request, the organisation does not have to reveal its plans to make him redundant if doing so would be likely to prejudice the conduct of the business (perhaps by causing staff unrest in advance of an announcement of the management's plans).

Negotiations with the requester

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.

Example

An individual makes a claim to his insurance company. The claim is for compensation for personal injuries he sustained in an accident. The insurance company dispute the seriousness of the injuries and the amount of compensation they should pay. An internal paper sets out the company's position on these matters and indicates the maximum sum they would be willing to pay to avoid the claim going to court. If the individual makes a SAR to the insurance company, they would not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

Regulatory activity

Some organisations may use an exemption from subject access if they perform regulatory activities. The exemption is not available to all organisations, but only to those that have regulatory functions concerning the protection of the public or charities, or fair competition in business. Organisations that do have such functions may only apply the exemption to personal data processed for these core regulatory activities, and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions.

For more detailed guidance on how this exemption applies, see ICO guidance on regulatory activity.

Legal advice and proceedings

Personal data is also exempt from the right of subject access if it consists of information for which legal professional privilege (or its Scottish equivalent, 'confidentiality in communications') could be claimed in legal proceedings.

The English law concept of legal professional privilege 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.

The Scottish law concept of confidentiality of communications provides protection both for communications relating to the obtaining or providing of legal advice and for communications made in connection with legal proceedings. Information that comprises confidential communications between client and professional legal adviser may be withheld under the legal privilege exemption in the same way that information attracting English law 'legal advice' privilege may be withheld. Similarly, the Scottish law doctrine that

a litigant is not required to disclose material he has brought into existence for the purpose of preparing his case protects information that, under English law, would enjoy 'litigation' privilege.

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.

It has been suggested that case law provides authority for organisations to refuse to comply with a SAR where the requester is contemplating or has already begun legal proceedings. The Information Commissioner does not accept this view, but he recognises that:

- the courts have discretion as to whether or not to order compliance with a SAR; and
- if a court believes that the disclosure of information in connection with legal proceedings should, more appropriately, be determined by the Civil Procedure Rules (the courts' rules on disclosure), it may refuse to order personal data to be disclosed (see chapter 11).

Nevertheless, simply because a court may choose not to order the disclosure of an individual's personal data does not mean that, in the absence of a relevant exemption, the DPA does not require you to disclose it. It simply means that the individual may not be able to enlist the court's support to enforce his or her right.

Social work records

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.

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 and education records

The exemptions that may apply when a SAR relates to personal data included in health and education records are explained in chapter 10 of the code.

Other exemptions

The exemptions mentioned in this chapter are those most likely to apply in practice. However, the DPA contains additional exemptions that may be relevant when dealing with a SAR. For more information about exemptions, see the ICO Guide to Data Protection.

An organisation that makes appropriate use of the exemptions in the DPA might have the following indicators of good practice:

Withholding or redacting information

If information is withheld in reliance on an exemption, the response explains, to the extent it can do so, the fact that information has been withheld and the reasons why. The explanation is given in plain English, and does more than simply specify that a particular exemption applies.

Information to be redacted is approved before source material is copied in a redacted form. It is then subject to at least one quality review by a manager to confirm that all data has been excluded appropriately. A copy of the disclosure bundle showing the redactions and the reasons behind them is retained for reference.

Once approved, redaction is either carried out manually using black marker which is then photocopied, or electronically using Adobe Acrobat or bespoke redaction software.

Ensuring consistency

Advice on applying the exemptions most likely to be relevant to the organisation's activities is included in SAR guidance for staff.

Quality assessments are carried out to ensure that exemptions are applied consistently.

10 Special cases

Credit files

There are special provisions regulating access to personal data held by credit reference agencies. Where credit reference agencies hold personal data relevant to an individual's financial standing (information in a credit reference file), they must provide a copy of the information within seven days of a written request and on payment of a £2 fee. Credit reference agencies will need to verify the identity of the person making the request before they respond. For more guidance about information held by credit reference agencies see Credit Explained.

Health records

What is a health record?

For the purposes of the Data Protection Act 1998 (DPA), a 'health record' is a record which:

- consists of information relating to the physical or mental health or condition of an individual; and
- has been made by or on behalf of a health professional in connection with the care of that individual.

'Health professionals' include registered medical practitioners, dentists and nurses and clinical psychologists. The DPA provides a full list of the types of professional that fall within the definition (see section 69 of the Act).

Information that forms part of a health record about a living individual is the personal data of the individual it relates to, regardless of the form in which it is held. This means that a subject access request (SAR) can be made for health records kept in manual form, eg on paper or in GP's medical notes wallets, as well as for health records kept electronically.

Can I charge a fee for providing subject access to health records?

You may charge a maximum fee of between £10 and £50 for complying with a SAR relating to health records. The precise amount of the maximum fee depends on how the health records are held.

- You may charge up to £10 for complying with a SAR relating to health records if they are held only electronically.
- You may charge up to £50 for complying with a SAR relating to health records if those records are held either wholly or partly in non-electronic form.

These charges may be made if you comply with the SAR by supplying the requester with a permanent copy of the relevant information. You may charge up to the relevant maximum fee regardless of the number of pages the information comprises.

However:

- if the health records in question fall into the second of the above two categories (that is, they are not exclusively electronic records and there is no intention to process them electronically), and
- they have been created or added to during the 40 days preceding the SAR

you must offer the requester the opportunity to inspect the manual records free of charge, rather than being provided with a permanent copy of them.

The amendment may have been either to the electronic or manual part of the record (or both). Assuming there is no intention to process the record electronically, access to the whole manual record will be free of charge. However individuals may tailor their SARs so that they relate only to information to which this right of free inspection applies, and you may also discuss with the individual whether or not they would agree to accept access only to information that is new or has been updated.

Are health records ever exempt from subject access?

The exemptions and restrictions that apply to other types of personal data also apply to personal data included in a health record. So, for example, if a health record contains personal data relating to someone other than the requester (such as a family member), you must consider the rules about third-party data before disclosing it to the requester (see chapter 7 for more information). However, information that identifies a professional, such as a doctor or social worker, carrying out their duties should not normally be withheld for this reason.

In addition, special rules apply where providing subject access to information about an individual's physical or mental health or condition would be likely to cause serious harm to them or to another person's physical or mental health or condition. These rules are set out in the Data Protection (Subject Access Modification) (Health) Order 2000 (SI 2000/413), and their effect is to exempt personal data of this type from subject access to the extent that its disclosure would be likely to cause such harm.

To apply this exemption, there clearly needs to be an assessment of the likelihood of the disclosure causing serious harm. Unless you are a health professional, you must consult the health professional who is responsible for the clinical care of the individual concerned before deciding whether the exemption applies. This requirement to consult does not apply if the individual has already seen or knows about the information concerned.

A further exemption from subject access to information about an individual's physical or mental health applies where 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.

Information held about pupils by schools

A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by a school. If the school is in England, Wales or Northern Ireland, the SAR should be dealt with by the school. If the school is in Scotland, the SAR should be dealt with by the relevant education authority or the proprietor of an independent school.

There are two distinct rights to information held about pupils by schools. They are:

- the pupil's right of subject access under the DPA; and
- the parent's right of access to their child's 'educational record' (in England, Wales and Northern Ireland this right of access is only relevant to maintained schools – not independent schools, English academies or free schools. However in Scotland the right extends to independent schools).

Although this code is only concerned with the right of subject access, it is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above, and also because 'educational record' is relevant when ascertaining the fee you may charge for responding to a SAR.

The statutory definition of 'educational record' differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record; eg, information about the pupil provided by the parent of another child is not part of the educational record.

Unlike the distinct right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent. For guidance about deciding whether a child is able to make their own SAR, see chapter 4. If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, you should clarify this before responding to the SAR.

In deciding what information to supply in response to a SAR, you need to have regard to the general principles about exemptions from subject access described elsewhere in this code. Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- information that might cause serious harm to the physical or mental health of the pupil or another individual;
- information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records; and
- certain information given to a court in proceedings concerning the child.

If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days. The maximum amount you may charge for dealing with the request depends on the number of pages of information to be supplied. The following table shows the maximum fees.

Number of pages of information supplied	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-59	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit for responding applies. The maximum fee for dealing with the request is £10.

Information about examinations

Special rules apply to SARs relating to information about the outcome of academic, professional or other examinations. These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results.

Information comprising the answers given by a candidate during an examination are exempt from the right of subject access. So a SAR cannot be used to obtain a copy of an individual's examination script.

Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a SAR for such information in cases where the SAR is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a SAR is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the DPA. So it would not be appropriate to refuse to provide details of examination marks in response to a SAR because the requester had failed to pay their tuition fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

11 Enforcing the right of subject access

The Information Commissioner's enforcement powers

Anyone who believes they are directly affected by the processing of personal data may ask the Information Commissioner's Office (ICO) to assess whether it is likely or unlikely that such processing complies with the Data Protection Act 1998 (DPA). This is called a compliance assessment.

If our assessment shows that it is likely that an organisation has failed to comply with the DPA (or is failing to do so), we may ask it to take steps to comply with the data protection principles. Where appropriate, the ICO may order the organisation to do so. However, the ICO has no power to award compensation to individuals – only the courts can do this.

The Information Commissioner may serve an enforcement notice if he is satisfied that an organisation has failed to comply with the subject access provisions. An enforcement notice may require an organisation to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence. The Information Commissioner will not necessarily serve an enforcement notice simply because an organisation has failed to comply with the subject access provisions. Before serving a notice he has to consider whether the contravention has caused or is likely to cause any person damage or distress. He can serve a notice even though there has been no damage or distress but it must be reasonable, in all the circumstances, for him to do so. He will not require organisations to take unreasonable or disproportionate steps to comply with the law on subject access.

The Information Commissioner has a statutory power to impose a financial penalty on an organisation if he is satisfied that the organisation has committed a serious breach of the DPA that is likely to cause substantial damage or distress.

For more information about the Information Commissioner's enforcement powers, see the ICO Guide to Data Protection.

Enforcement by court order

If you fail to comply with a subject access request (SAR), the requester may apply for a court order requiring you to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

The courts have indicated that, where other legal proceedings are contemplated or in progress, they may be reluctant to allow individuals to use the right of subject access as a means of accessing information in connection with those proceedings where disclosure should more appropriately be dealt with under the Civil Procedure Rules. The courts may even regard an application for an order under the DPA as an 'abuse of process' if the application would not have been made but for the desire to access information to be used in other legal proceedings. Nevertheless, as we explained in chapter 9, whether or not a court would be likely to grant an enforcement order has no bearing on your legal duty to comply with a SAR. You may only refuse to comply if a relevant exemption under the DPA applies in the particular circumstances of the request.

Awards of compensation

If an individual suffers damage because you have breached the DPA – including, of course, by failing to comply with a SAR – they are entitled to claim compensation from you. This right can only be enforced through the courts. The DPA allows you to defend a claim for compensation on the basis that you took all reasonable care in the circumstances to avoid the breach, but it is likely to be difficult to establish this defence where you have failed to respond to a SAR within the prescribed time limit, or where you have not provided the requester with all the information to which they are entitled.

For more information about claims for compensation, see the ICO Guide to Data Protection.

Appendix – Subject access request checklist
Ten simple steps to understanding subject access requests

1. Is it a subject access request?

YES **Go to question 2**
NO Handle as part of your normal course of business.

Any written request by an individual asking for their personal information is a subject access request. You can choose to deal with it in one of two ways: as a routine enquiry, or more formally.

If you can, treat requests that are easily dealt with as routine matters, in the normal course of business; for example:

- How many cash withdrawals did I make from my account last month?
- What is my customer reference number?

The following are more likely to be treated formally:

- Please send me a copy of my staff records.
- I am a solicitor acting on behalf of my client Mr X and request a copy of his medical records. Appropriate authority is enclosed.

2. Do you have enough information to be sure of the requester's identity?

YES **Go to question 3**
NO Ask the requester for any evidence you reasonably need to confirm their identity.

3. Do you need more information from the requester to find what they want?

NO **Go to question 4**
YES Ask them **promptly** for the other information you reasonably need so you can find the information they want.

4. Are you charging a fee?

NO **Go to question 5**

YES You will need to ask the individual **promptly** to pay the fee.

The maximum fee you can charge is £10, unless the requested information is medical or education records – see chapter 5 for more on this.

The 40 calendar days in which you must respond starts when you receive the fee and all the information you need to help you find the information.

5. Do you have the information the requester wants?

YES **Go to question 6**

NO Tell the requester you do not have the information they want.

6. Will the information be changed between receiving the request and sending the response?

NO **Go to question 7**

YES You can still make routine amendments and deletions to personal information after receiving a request.

You must not make changes to records as a result of receiving the request, even if the information is inaccurate or embarrassing.

7. Does it include information about other people?

NO **Go to question 8**

YES You will not have to supply the information unless the other people mentioned have given their consent for the disclosure, or it is reasonable to supply the information without their consent.

If you decide not to disclose the other people's information, you should still disclose as much information as possible by redacting the references to them. See chapter 7 for further guidance on this.

8. Are you obliged to supply the information?

YES **Go to question 9**

NO If all the information that the requester wants is exempt from subject access, then you can reply that you do not hold any of their personal data that you are required to reveal.

There are some circumstances when you are not obliged to supply certain information.

See chapter 9 for guidance on the exemptions.

9. Does the information include any complex terms or codes?

NO **Go to step 10**

YES You must make sure you explain the codes so that the information can be understood. **Go to step 10**

10. Prepare the response

You must provide a copy of the information in a permanent form unless the individual agrees otherwise, or doing so would be impossible or involve disproportionate effort.

See chapter 8 for more detail.

If you would like to contact us please call 0303 123 1113

www.ico.org.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

February 2014
Version 1.1

Information Commissioner's Office