Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Subject access requests: Introduction

Under the Data Protection Act 1998 (DPA), an individual is entitled to ask an organisation if it holds information relating to him/her (i.e. his/her *personal data*) and ask for a copy of it to be supplied to him/her. This is known as making a subject access request (or a *SAR*).

This guidance is for any member of DfE staff who receives such a request. Some sections reflect the department's statutory duties, others offer practical advice on how to handle and respond to a SAR.

All SARs need to be considered on a case-by-case basis and with the support of the Data Protection Team in Privacy and Information Rights Advisory Service (PIRAS) in the Legal Adviser's Office (LAO).

With a statutory deadline within which to respond to subject access requests, we ask that you notify us as soon as you receive a request for personal data. This will enable us to advise you in good time and monitor the progress of the request you are handling.

Please contact relevant colleagues in the Data Protection Team for any advice regarding the handling of requests covered by this guidance.

1. Receiving a request for personal data

The Data Protection Team maintains a log of all SARs received by the department so please notify us as soon as you receive a request. For monitoring purposes and to assist you, we need;

- the name of the requestor
- the date the request was received by the Department (not your team); and
- the wording of the request (ideally, by sending us a copy of it)

Personal data is information about a living person from which that person can be identified and includes any expression of opinion about him/her or any indication of intentions towards him/her. It might appear in electronic and/or paper records, internal notes, recorded telephone conversations and/or CCTV footage.

A requestor (or 'data subject') does not need to use the term, 'subject access request', or mention the Data Protection Act, for us to consider their request for access to their personal data.

SARs are not generally stored on ECHO; they are forwarded to the relevant team(s) holding the requestor's personal data. If a SAR appears within correspondence addressing other matters (which require a response via ECHO), this correspondence

can usually be stored on ECHO but any personal data to be released (in response to the SAR) will be provided outside of the ECHO system, with a copy of what is released held locally.

To comply with the DPA, our responses to SARs must be made within 40 calendar days of them being received by the department, i.e. not just the handling team. This is why it is important that SARs are received by the handling team as soon as possible.

It is departmental policy to take the first day by which we start counting this 40 day deadline as the day *after* the request has been received (i.e. the first full day that we have to work on it).

Under an individual's *subject access rights* s/he is entitled to be:

- informed whether we hold any of their personal data and where (i.e. by which team) it is being held/used

- given a description of the purpose(s) for which their personal data is being used as well as any information as to the source and recipients of this personal data

- provided with a description of their personal data, along with a copy of it in an intelligible and permanent form (subject to relevant exemptions)

Upon receipt of a SAR, the team handling it must nominate an individual (from within that team) to handle the request and provide its response. This should be someone who is either familiar with the individual making the request, corresponded with them in the past or has experience of handling information relating to them.

If personal data in scope of a SAR is held by *more than one* team, PIRAS will co-ordinate the handling of the request and identify the team most suitable to provide a response on behalf of the department. In such situations, each team holding personal data, relating to the requestor, will manage their own parts of the request.

2. Charges

DfE (including its agencies) does not charge for responding to subject access requests so any money accompanying SARs must be returned to the requestor with a covering letter explaining this. Details of the amount received, the requester's name, cheque number, date received and returned must all be logged.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Clarifying details and/or confirming the ID of the requestor

1. Interim responses to the requestor

Given the statutory deadline within which to respond to a SAR, any clarification required from the requestor must be sought, in writing, at the earliest opportunity. Any person tasked with handling the request is responsible for sending any interim responses. These should include notification that the enquiry is going to be considered under the terms of the Data Protection Act.

Any initial response should also mention that the department expects to supply a full response as soon as possible and, in any event, within the statutory deadline of 40 calendar days. Before your work on a SAR can begin, you must be sufficiently confident that you:

- understand the request
- are able to confirm the identity of the requestor (and that they are entitled to the information they are requesting)
- understand what personal data is being requested; and
- are confident that you hold the requested information

If any of the above remains unclear, or requires further clarification, it is essential that you respond to the requestor for further information/confirmation at the earliest opportunity.

Material in scope of SARs can vary, ranging from requests for specific personal data (i.e. narrow in scope, linked to a specific issue or within a certain time period) to requests of a broader nature (e.g. a request for *all* personal data, relating to the requestor, held by the department).

2. Seeking clarification and how it affects the 40 day deadline

Once you have sought clarification/confirmation from the requestor, the 40 day countdown is ‘paused’ from this point until you receive the necessary clarification from him/her. It is for this reason that, to limit the amount of lost time, you seek this clarification/confirmation as soon as you are able.

For example:

1 May: Request received and allocated to you
You decide that you need further clarification of the request or proof of ID (or both).

2 May: Day 1 of the 40 day deadline
Note: This is still considered day 1 if this is a non-working day.

8 May: You request further information
You write to ask for further information. The counting down of your 40 day deadline now 'pauses'. You have used 7 of your allocated 40 days (i.e. 2nd – 8th May). Upon receipt of the requested further information, you will still have 33 days within which to respond (unless you need additional clarification).

12 May: You receive the requested information
The 'counting down' of the deadline (now standing at 33 days) resumes from 13th May (the next full day), providing you with a final deadline date (at this point) of 14 June.

If the last day of your 40-day deadline falls on a Saturday, Sunday or Bank Holiday, your response will need to be sent out on the last working day prior to this non-working day.

3. Confirmation the request or the identification of the requestor

If a SAR has been allocated to you for a response, this is most likely to be because the requestor is known to you, you have corresponded with them before or you are responsible for processing personal data relating to them.

If you do not know what personal data the requestor is requesting, you are able to contact them and ask them to specify what information they are asking for and/or where, in the department, they think it is being processed.

Before you start working on the SAR, it is also important that you have confirmed the requestor's identity, current address and that they are entitled to the requested information. This is because it is unlawful to make personal data available to anyone who does not have a right to see it.

If confirmation of ID *is* needed, it is advisable to first consider whether you/your team/anyone else in the department already holds information which will enable you to confirm that:

- the requestor *is* who they say they are

- they are legally entitled to see the personal data they are requesting
- you know where to send the requested data

Your team may have recently been corresponding with the requestor (and at the address provided in the SAR) or you hold sufficient other relevant information (about the requestor) from which it's possible to confirm the requestor's identity.

If you have been content to correspond with the requestor, up until the point they make their SAR, it would seem inconsistent to now ask them to confirm that they are who they claim to be.

If you feel unable to confirm a requestor's ID, either from the request or information you already hold, it will be necessary to ask the requestor to provide you with further information to assist you with this. There are a number of suitable documents that can be requested for identification purposes, these include a photocopy of one of the following:

- the relevant parts of the requestor's driving licence
- a recent gas, electricity or telephone bill addressed to him/her
- a council tax bill which names him/her; and, if necessary
- a bank statement addressed to him/her

It is important to note that these must have been addressed to the requestor at their current residence (as identified in their request).

In most cases, a copy of only one of these documents will be required and, in the case of utility bills or bank statements, it is not necessary for you to see any of the financial details they contain. We therefore suggest that you advise the requestor to black out these parts, prior to sending to the Department, if s/he doesn't want you to see them.

If the request is being made by a parent on behalf of a child, you will also need to confirm that the requestor is entitled to the information in scope of the request (see further guidance below). How you do this needs to be considered on a case-by-case basis with the advice of the Data Protection Team.

If you are unable to confirm the identity of the person making the request, you cannot comply with it and no comments concerning the requested personal data can be made. You will, however, be expected to provide a reasonable level of assistance to the requestor in order to try to establish their identity and what it is they would like released to them.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Important considerations

1. The release of personal data to third parties

When responding to a SAR, personal data should never be sent to anybody other than the data subject (i.e. the requestor) unless they have nominated an agent (such as a friend, spouse, parent, partner or legal representative) to act on their behalf.

Ensure that you have sufficient information to confirm that the request is genuine and that the data subject has given their consent for the department to receive the request from/provide the response to a third party.

Requests for personal data relating to a child who does not have sufficient maturity to understand the SAR process (or any personal data which would be made available to them) may be made by a parent/guardian on their behalf. In such cases, it is still be necessary to consider whether the request is genuine and that the requestor (acting on behalf of such a child) is entitled to the personal data being requested.

2. Repeat requests

Organisations are not obliged to respond to the same or similar requests, made by the same requestor where a response has already been made (or the requested information isn't held). If a SAR is the same (or sufficiently similar) to a previous one, and no further (new) personal data is available for release, you do not need to process the request again.

If more than six months has elapsed between SARs, a copy of the originally supplied SAR material may be provided at your discretion.

If there is *new* personal data (belonging to the requestor) in scope of the SAR which can now be made available (i.e. because it has been updated or it was not held at the time of an earlier request) only this new personal data needs to be considered for release in response to the later request (subject to any other relevant exemptions).

3. Responding to requests for personal data relating to children

a) If the request is made by the child

The DPA does not specify an age at which a child can independently make a request for their personal information but you need to take into account whether:

- the child properly understands what is involved in making such a request; and/or
- s/he wants his/her parent (or someone else) to be involved by acting on his/her behalf

The Information Commissioner's Office (ICO) suggests that a child of 12 or above is expected to be mature enough to understand the request they are making but that some children may either, (a) be sufficiently mature at an earlier age or (b) lack sufficient maturity until a later age. Requests from children should therefore be considered on a case-by-case basis, based on what you know about the child.

Consider (as far as possible) whether the child in question is/will be able to understand the request and the personal data relating to them that the department holds. Under a child's own data protection rights, a guardian/parent will only be able to see information about that child if s/he is unable to act on her/his own behalf or s/he gives consent for a parent/guardian to have access to their personal information.

b) If the request is made by a parent/someone else acting on behalf of a child

It is important to ensure that the request has been made by someone who has a right to see the personal data being requested. It might be possible to confirm this relationship from what you already know about the requestor/child from other information you already hold.

If the child is over the age of 12, you might feel it is necessary to consider seeking his/her consent before releasing any information about him/her to the requestor. If you are unable to confirm the requestor's right to access the child's personal data, it will be necessary to ask them to provide proof of their relationship with the child.

As a minimum, we would expect a parent/legal guardian to be able to provide you with the child's full name, date of birth, home address and the name of their school. In most cases, this information can be confirmed by records held on the National Pupil Database (NPD), managed by Data Services Division.

Even if the requestor is unable to provide you with these details, you still need to consider whether the request is genuine (and that the requestor is entitled to the requested information).

Further proof might come (for example) in the form of a copy of a Child Benefit letter (carrying the name of the requestor as well as that of the child) or other suitable documentation. It is not necessary for you to see any financial details in such documents so the requestor can be advised to blank these parts out before sending copies to you if they do not want you to see them.

If further advice is needed with regard to any of the above, please contact the Data Protection Team in PIRAS.

4. Requests for personal data made by DfE staff/ex-DfE staff

DfE's Human Resources Division co-ordinates and responds to subject access requests made by current/ex-members of DfE staff. Such requests need to be made in writing, either by letter or email to HR at:

[redacted]

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Gathering material in scope of a SAR

Once you have confirmed that it is a request for personal data, data in scope of the request, the identity of the requestor and their eligibility to see the requested information, there is a need to locate the requested personal data. This location may already be known to you but, for the purposes of handling a request of a broader nature, you may be further required to search all of your systems in order to locate the requested information.

Searches may include (for example) trawls of electronic and hard copy materials in a team's shared area, online Workplace, staff F:Drive(s) and correspondence relevant to cases held on ECHO/IRIS. Relevant information should be collected, collated and forwarded to the person responsible for handling the request.

This person will then need to consider whether the material held falls in scope of the request and consider what the requestor is entitled to have made available to him/her under the DPA and prepare it for release (or redact as necessary).

1. Sifting material which falls within scope of a request for personal data

The DPA defines personal data as, '*…data which relate to a living individual who can be identified:-*

- *from those data; or*
- *from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.' (s.1 (1))

In order for information about a person to be classified as personal data, the individual has to be:

- the focus of the information; and that
- information has to tell you something of significance about that person

Information which *'relates to'* an individual can also constitute personal data. When considering whether information relates to an individual, consider whether you (or anyone else) would be able to make a connection between that information and the requestor either from the information alone or from that information when placed alongside additional information that the department holds (or is likely to receive).

It is the responsibility of the team handling the SAR to:

- identify personal data appearing in any documents it holds (or has access to via ECHO or shared areas); and
- prepare it for release

You will be expected to identify personal data, relating to the requestor, that you plan to release as part of your response as well as any personal data you consider needs to be withheld under relevant exemptions appearing in the DPA.

For the purposes of identifying personal data you hold, you must only include personal data being held/processed at the date the SAR was received and not include any personal data created/processed after that date/time. This means, for example, personal data appearing in correspondence between you and PIRAS concerning how to handle the SAR should not form part of your response.

For more practical advice on how to sift material to identify personal data, please contact the Data Protection Team in PIRAS.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Considering third party personal data

Whilst the DPA gives individuals the right to request access to information about them that we hold, it does not entitle them to information we hold which identifies third parties. Such 'third party personal data' is information relating to any person other than the data subject (i.e. the requestor) or any employee of the department. For the purposes of the DPA, departmental employees (or anyone acting on our behalf) are not considered third parties.

Third party personal data might be linked to a requestor's personal data in terms of:

- the third party being identifiable as the *source* or *recipient* of the requestor's personal data; or
- the third party being *identifiable* from information we hold which falls in scope of the request

1. Disclose of third party personal data to the requestor

Information should not be withheld from an individual purely based on the criteria that it constitutes third party personal data. Where information that falls in scope of a SAR *does* (or might) lead to the identification of a third party, the requestor's right of access to his/her personal data must be weighed against (a) the third party's right to privacy and (b) any duty of confidentiality that might exist between the department and the third party.

As a general rule, third party personal data should not be disclosed to a requestor unless:

- the third party has consented to the disclosure to the data subject; or
- it is reasonable in, all the circumstances, to disclose it without the consent of the third party

If you are remain unsure whether to release/withhold third party personal data, consider whether:

- the information you are making available will enable the requestor to identify that third party
- it would be unreasonable, in the circumstances, to release the third party personal data to the requestor and whether to do so might breach the third party's data protection rights
- the requestor already knows the information about the third party anyway
- there would be a reasonable expectation that information provided (which will identify a third party) was provided in confidence

If the third party is not known to the requestor and it would seem unfair or unreasonable to make the third party's personal data available to him/her, you should consider withholding this personal data from release.

However, if you feel that the release of third party personal data is unlikely to breach a third party's data protection rights, and it seems reasonable in the circumstances to release their personal data to the requestor, you may wish to release this third party personal data at your discretion. In certain circumstances, for example, it might seem reasonable to release third party personal data to the requestor in cases where that third party personal data is already known to the requestor.

Decisions as to whether to withhold/release third party personal data can be particularly complex. If you need any assistance with this, please contact the Data Protection Team in PIRAS for advice.

2. Identifying DfE staff/releasing staff names in SAR responses

When responding to SARs, it is the department's policy to release information which identifies DfE staff (irrelevant of grade) where they have public facing roles and/or are already known to the requestor. It may be, for example, that these staff have corresponded with the requestor in the past and/or are already known to have been involved in their case, complaint etc.

In cases where members of staff do not have a public facing role and are not already known to the requestor, it is the policy that the names of senior civil servants (i.e. of Deputy Director grade and above) are usually released and the names of more junior staff withheld.

If it is felt that the release of a member of staff's name might put his/her safety, health or well-being at risk then consideration should be given to withholding his/her name from the requestor. Please contact the Data Protection Team in PIRAS for advice if you think this might be the case.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Exemptions available under the Data Protection Act

There are certain exemptions to a data subject's right of access to his/her personal data and these are outlined below. These can only be relied upon in certain circumstances, should be applied on a case-by-case basis and cannot necessarily be applied to withhold entire documents from release (i.e. and only to the relevant personal data within such documents).

In order to apply an exemption, you will also need a robust reason for doing so and be prepared to defend your decision to apply it (to PIRAS, the ICO and/or in court if necessary). You must therefore record your decision, the exemption(s) being applied (and to what information) and your reasons(s) for applying it/them.

Not all DPA exemptions are relevant to the work of our department or its agencies. The following are the most common exemptions on which we sometimes rely:

- Crime and taxation (s29(1) of the DPA)
- Research, history and statistics (s33)
- Regulatory activity (s31); and
- Legal professional privilege (Schedule 7(10))

Crime and taxation (s.29 (1))

Under the crime and taxation exemption, personal data may be considered exempt from release if personal data is being processed (by ourselves or others) for the purposes of the:

- prevention or detection of a crime; and/or
- apprehension and/or prosecution of offenders

where the release of the personal information would be likely to prejudice such matters.

Consideration should therefore be given to withholding such personal data if it might, on its release, enable the data subject (or another individual to assist the data subject) to avoid apprehension or prosecution or where the release of personal data could prejudice an investigation in any other way.

Research, history and statistics (s.33)

We are not required to release personal data in response to a subject access request if that personal data has been collected and used for research, historical and statistical purposes and:

- at the time of collection, the data subject was made fully aware of the use(s) of their personal data (in the form of a privacy notice)

- the personal data has been/is only being used for the purposes for which it was collected and will not be used to support any decision relating to the data subject
- the results of the research will be/have been anonymised in any published information

Regulatory activity (s.31)

If there is any possibility that a disclosure of personal data could prejudice a function of the Secretary of State/our department or its agencies, you should consider withholding the relevant personal data under the regulatory activity exemption. As with the use of other exemptions, you must have a robust argument for applying this exemption.

The DPA contains a list of the type of the relevant functions for which this exemption can be applied, one of which is designed to protect members of the public against seriously improper conduct by, or due to the unfitness or incompetence of, persons authorised to carry out any profession or other activity.

The type of information which might fall under this exemption might therefore appear in:

- advice given by an advisory panel to the Secretary of State
- internal communications between our officials and an advisory panel
- recommendations and comments of officials in submissions to the Secretary of State

This exemption will only apply in a very limited number of circumstances and you will only be able to withhold that information which is likely to prejudice a regulatory function.

As with other exemptions, it cannot be applied in a 'blanket fashion' (i.e. by applying it to all documents you hold or to entire documents within which the relevant information appears) but only those parts of the documents, the release of which could potentially prejudice the functions of the Secretary of State and/or the department or its agencies.

Legal professional privilege (Schedule 7(10))

Personal data that appears in:

- a request for legal advice; and/or
- legal advice provided by a legal adviser

may be considered exempt from release on the grounds of client confidentiality. This exemption can only usually be applied if the advice was sought in relation to actual or potential legal proceedings.

Exemptions available under secondary legislation

In very rare circumstances, secondary legislation might apply to the type of personal data you hold. If you feel that personal data you process is captured by exemptions under the following statutory instruments, please contact the Data Protection Team in PIRAS for further advice.

The Data Protection (Subject Access Modification) (Health) Order (SI 2000/413)

There is often a misapprehension that all health information held by an organisation is exempt from release under the DPA. This is not the case.

An individual's health information *might* be exempt from release if access to it is likely to cause serious harm to the physical or mental health of the data subject or any other individual. However, you are advised not to withhold health information concerning a data subject in cases where this information is already known to him/her.

Please note though that, any decision as to whether release of personal might cause such harm can only be made by an appropriate health professional responsible for the care of the data subject and not DfE staff.

The Data Protection (Subject Access Modification) (Education) Order (SI 2000/414)

As with health information (see above), personal information relating to a school pupil that constitutes an educational record may be exempt from release in response to a SAR if providing access to it is likely to cause serious harm to the physical or mental health of the data subject or any other individual.

The statutory definition of a pupil's educational record is set out in the Pupil Information Regulations 2005. Whilst the department does not routinely receive or maintain copies of educational records, it is possible that one might be supplied to a team for the purposes of responding to a complaint about a child's education.

The Data Protection (Subject Access Modification) (Social Work) Order (SI 2000/415)

This instrument applies to personal information relating to social work records which have been obtained from a wide range of bodies. These include;

- local authority social services
- local education authorities (in their position of ensuring children receive a suitable education)
- health authorities, NHS trusts or health boards

It is highly unlikely that staff within our department (or any of its agencies) will have ready access to personal information which appears in social work records, it is possible that certain teams may be supplied with such information in order for them to carry out their functions.

Please contact the Data Protection Team if you feel this exemption applies to the records you hold in scope of a SAR.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Redacting information to be withheld from release

Where you need to withhold information from a data subject (either because it is personal information which is exempt from release under the terms of the DPA or constitutes personal data relating to a third party), such material is withheld via a process called *redaction*.

Redaction is the practical method of withholding parts of a document that an individual is not entitled to see. It can be carried out in a variety of ways but, for documents held in hard copy, the most common approach is to cover the information to be withheld with an opaque marker pen or correction tape. Marker pens, printer inks and types of paper vary in quality and this sometimes makes it difficult to successfully redact words printed on paper.

When working with editable electronic documents, it is our policy to advise that information to be withheld is removed from the document and replaced with a series of 3 dots.

1. Redacting information appearing in hard copy materials

Original source material should never be used for redaction purposes, unless it is a printout of a document that you hold electronically.

For documents that you only hold in hard copy, we advise that you make single-sided photocopies of these and place the original(s) in a secure place. On the copy, highlight all information which you think needs to be withheld from the data subject (on the grounds that it is either third party personal data or personal data to which an exemption applies).

If you need our advice on your handling of the request, you can scan this highlighted version and send it to us for comment.

Once you are content with your highlighted version, you will need to produce a version which you can make available to your requestor (with the highlighted information suitably redacted). For this purpose, make another copy of the original and redact that information which you previously identified for redaction with highlighter in your alternate version.

This process then leaves you with three versions; the original document(s), a second set (with yellow highlighting, to show information that you plan to withhold) and a third version (with that material redacted). The third version (a photocopy or printed PDF of it) is the one to be supplied to the requestor.

A simple test to see whether the redaction process has been successful is to hold the document up to the light/at a window to see whether it is still possible to read what sits behind the redacted areas. If it is possible to read/decipher any of the text

to be withheld, this is not sufficient and further attempts must be made to obliterate this information.

If the majority of the source material needs to be redacted, it may be more practical/appropriate to transcribe the personal data from the source material and place it in a separate document. This should only be considered in cases where the requestor would receive a large volume of material, most of which is redacted. In such cases, please contact us for advice.

2. Redacting information which appears in electronic materials

a. Emails

Where a requestor is entitled to personal data appearing in emails, you will need to copy them into a Word document. In order to capture the entirety of an email (i.e. to ensure you include the *From*/*Sent*/*To* and *Subject* fields), you will need to prepare the relevant emails/email chains for forwarding.

Opening an email and clicking on the '*forward'* icon on your Outlook toolbar, enables you to copy and paste the entire email (including the *From*/*Sent*/*To* fields) into a Word document. Once transferred to a Word document, you can treat the contents of emails/email chains in the same way you would any other Word document.

b. Word documents

As with hard copy versions, highlight any text which needs to be withheld from release. In considering your handling of your response, you can also make comments (in Tracked Changes) to explain reasons for withholding material or to ask us questions when seeking advice/clarification.

Once happy with your proposed redactions, your version with highlighting (and any comments) can then be saved as a record of the SAR process (you might want to save it with the name such as, *SAR response for [data subject's initials] HIGHLIGHTED)*.

From your highlighted version, a new version can be created/saved (under a new name) in which those parts to be withheld are deleted and replaced with three dots (i.e. '…'). This is the version that you will print off and supply to the requestor. Where *names* are to be redacted from the *From/To* fields of emails, we suggest that these are redacted (in black) instead of replacing with a series of dots.

This will then leave you with three electronic versions; the original, a version containing highlighted redactions and a final version in which any withheld information has been redacted (by being replaced by a series of dots).

As the volume, type and format of material in scope of a SAR vary from one request to another, it is advisable to contact us for advice on the most practical way of redacting information as part of a SAR response.

c. Excel workbooks/spreadsheets

These can be redacted in the same way as Word documents but, for some requests, it may be beneficial to copy and paste relevant headings, along with the personal information to be released, from the spreadsheet that you hold and paste it into a fresh workbook/spreadsheet. This will help to avoid inadvertently printing off and releasing personal information relating to third parties.

Handling requests for personal data (subject access requests) under the Data Protection Act 1998 (DPA)

Releasing non-personal data for context and preparing your response

1. Contextual information

Whilst the DPA entitles an individual to access to his/her personal data, it does not entitle them to entire documents within which that personal data appears. However, for openness and transparency, you are encouraged to release non-personal data where it is relevant to/provides context of the personal data you plan to release.

It is important to ensure that any non-personal data that you do plan to release still falls within scope of the request you are handling and that you consider any expectations you feel the requestor may have, in terms of what he/she will receive as part of your response.

Although the release of such information will be at your discretion and outside of the DPA, it must still comply with the terms of the DPA. It should not (for example) contain third party personal data (the release of which might breach that third party's data protection right) or personal data (relating to the requestor) that you consider should be withheld from release under a suitable exemption.

2. Preparing your response

It is the department's policy to release as much information to the requestor as is relevant, practicable and lawfully allowed. As personal data is to be provided in hard copy format, it should take the form of printouts and/or photocopies of original documents with relevant information (to which the requestor is not entitled) neatly redacted.

Your response to a SAR must contain:

- a copy of the personal data in scope of the request
- a covering letter, outlining where the requestor's personal data is currently located and the purpose(s) for which it is being held/used
- a description of the personal data being released, it's source, any recipients; and, where necessary
- a description of any exemptions relied upon to withhold personal data relating to the requestor (except in cases where to make this known might prejudice a criminal investigation)
- a glossary explaining any acronyms and jargon which appear in the personal data, the meanings of which might not be clear to the requestor

Please note that, whilst the inclusion of schedule (listing the material within which the requestor's personal data appears) is helpful, this is not a requirement. Whilst this is good practice (and to be encouraged), we would only expect this if time allows and would discourage you from doing so if it is going to cause undue delay to your response.

3. Suggested lines for response letters

We do not provide templates for acknowledgement or response letters because of the varying nature of the type of requests the department receives. The paragraphs below may prove useful when corresponding with a requestor and there is scope to alter the wording of these (either to suit the nature of the request or your own writing style).

Please contact us if none of the examples provided below apply to the request you have received and/or you with need us to draft relevant data protection lines for your response.

a) For acknowledging a request

The following paragraphs may be suitable for an initial acknowledgement or a final response (i.e. cover letter) if not stated previously:

> *Thank you for your [letter/email], dated [insert date], requesting [describe what has been requested] which I [am treating/have treated] as a subject access request for personal data made under the Data Protection Act (DPA).*
>
> *Personal data is information about a living person from which that person can be identified and includes any expression of opinion about him/her or any indication of intentions towards him/her.*
> *Whilst the DPA gives you the right to see certain information (i.e. your personal data), it does not require us to provide you with whole documents that contain this information. You are also not entitled to see: information which does not constitute your personal data; personal data belonging to others (where to release this data could infringe their data protection rights) or personal data belonging to you that is exempt from release to you under the terms of the Act.*
>
> *The DPA requires us to comply with your request for information promptly and, in any event, within 40 days from the date of receipt of your written request. We received your request on [insert date]. We aim to send you copies of all personal data that you are entitled to see under the terms of the DPA as soon as we can, without undue delay, and within the statutory deadline.*

b) Asking for ID and/or clarification of the information being requested

Consider including the following paragraphs if it is unclear where the department holds the requested information and/or if the requestor's identity cannot be authenticated either from information already held in DfE records/supplied by the requestor and/or where it is unclear what the requestor is asking for.

When it is unclear where, in the department, the requestor's personal data is held:

> *Under section 7(3) of the DPA, we can ask you to let us have further information to help us locate the information you want.*
>
> *I would be grateful if you could indicate where in this department you think your personal data is being processed. If you do not know, I would be grateful if you could tell me if you have had any direct dealings with this department and, if so, the person or team you have dealt with.*
>
> *Please supply the above within 40 days. If I do not hear from you within this time, I will assume that you no longer require the information you have requested. If you have any queries about this letter please contact me using the details at the top of this letter.*

If you need to confirm the identity of the requestor:

> *In order to confirm your identity, I must request information from you to satisfy ourselves of your identity. This is to ensure we only supply personal data to someone who has a right to see it.*
>
> *For this purpose, can you please supply me with proof of your identity and address by sending me a photocopy of one of the following:*
>
> - *the relevant page of your passport or driving licence showing your name and address; or*
> - *a recent utility or council tax bill showing your name and address*
>
> *Please supply the above within 40 days. If I do not hear from you within this time, I will assume that you*

> *no longer require the information you have requested. If you have any queries about this letter please contact me using the details at the top of this letter.*

4. Sending your response

When responding to a SAR, personal data must **not** be sent by email over the Internet (i.e. outside of the GSI network) as this is not regarded as a secure method of delivery. In some cases, the large volume of personal data to be released would also make electronic delivery impractical.

Responses must be made in hard copy format and posted by Royal Mail Special Delivery in line with guidance provided by the Departmental Security Unit (DSU). For added security, your response should be double enveloped (with the requestor's name and address on both envelopes and you should write, '*Royal Mail Special Delivery'* on the outer envelope.

We advise you to physically take the response to your local DfE post room. Once there, it is advisable to make postal colleagues aware that your letter/package needs to be delivered by Royal Mail Special Delivery.

If there is no personal data to be released as part of the SAR response (i.e. the Department does not hold any personal data belonging to the requestor), a response explaining this can be sent by email or by standard Royal Mail post.