Child and Adult Services
Subject Access Requests Guidance

This Guidance is not applicable to Access to Information requests about Adoption. For requests about Adoption please consult the Adoption and Children Act 2002 or contact the Family Placement Team.

1. Introduction

A Subject Access Request (SAR) enables individuals to find out what personal data we hold about them, why we hold it and who we disclose it to.

Individuals have a right to be told on request:

- Whether we have personal data about them
- What the personal data is used for and the reasons it is being used
- Whether and to whom it might be given to
- Where the data came from
- The logic of any automated decisions taken about them such as a computer generated decision to grant or deny credit.

Some types of personal data are exempt from the rights of subject access and so cannot be obtained by making a SAR. More details on exemptions will be outlined later.

The processing of personal data by Hartlepool Borough Council (HBC) is essential to many of its services and functions. Compliance with the Data Protection Act 1998 (DPA) will ensure that this processing is carried out fairly and lawfully. The DPA seeks to strike a balance between the needs of an organisation to function effectively and efficiently and the respect for the rights and freedoms of an individual.

HBC is committed to a policy of processing personal data within the law and ensuring that information about individuals is collected and used fairly, stored safely and securely and not unlawfully disclosed to any third party.

Responding to SAR's provides us with an opportunity to improve our customer service and service delivery by ensuring that we maximise the quality of the personal information we hold and act in an efficient and transparent way.

The process for responding to SAR's has been developed in line with the Information Commissioner's Officer (ICO) "Subject Access – Code of Practice" (2014) and complies with HBC's Information Security Policies and will follow the Code of Practice contained in the standard ISO17779 (Information Security Management) where appropriate.

2. Acceptable Requests

- An SAR must be made in writing, whether manual or electronic.

- The request does not have to be in any particular form or use the works Subject Access Request. A request is valid if it is clear that the individual is asking for their own personal data.
- HBC do have a Subject Access Request form and it can be useful to signpost the individuals to that form because that will make it easier for the individual to include all the detail we might need in order to locate the information they want. However, they do not have to use the form and the Local Authority/Public Body cannot use signposting to the form as an excuse to extend the timescale to complete the request.
- SARs can be made and should be accepted via social media or via third party web sites.
- SARs which are not in writing can be accepted in certain circumstances, e.g. if there is a language barrier or the individual has a disability.
- The requester does not have to tell us the reason for making the request or what they intend to do with the information requested.
- A request is valid regardless of where it is received in HBC.
- Requests can be made via a third party e.g. a solicitor or anyone else identified by the individual whose data it is. We do need to be satisfied that the third party is entitled to act on behalf of the individual and it is the third party's responsibility to provide evidence of this.

2.1. Requests for information about children.

Whatever the age of the child, data about them is still their personal data and does not belong to anyone else such as a parent or guardian. It is the child who has a right of access to the information held about them and you have to decide if the child is able to understand (in broad terms) what it means to make a SAR, how to interpret the information they receive as a result of doing this and the potential impact on them from seeing the records.

You need to take into account:

- Where possible, the child's level of maturity and their ability to make a Subject Access Request, the complexities involved in that decision and the possible consequences of their decision;
- 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.

2.2. Subject Access Requests by Third Parties

If the individual feels more comfortable allowing someone else to act for them, HBC may receive a Subject Access Request via a third party on behalf of an individual. 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. Third party requests might be a written authority or it could be a more general Power of Attorney.

To reiterate, the onus is on third party acting on behalf of an individual to convince HBC they are entitled to act on behalf of that individual.

If you as Data Controller think an individual may not understand or be fully aware of what information would be disclosed to the third party requesting on their behalf, it may be advisable to contact the individual before you send the information to the third party. Once the individual has reviewed the information it is then their choice whether or not HBC discloses the information to the third party.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the DPA or in the Mental Capacity Act 2005 enabling a third party to exercise Subject Access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters by the Court of Protection.

3. What is Personal Data?

Personal Data is information that relates to a living individual who can be identified either:

- From the information; or
- From the information combined with any other information which is already in the possession of, or likely to come into the possession of, the person or organisation holding information.

The information includes any expression of opinion about the individual, and any indication of the intentions of the HBC employee or any other person in respect of the individual. Personal data will therefore cover basic details such as name, address, date of birth and telephone numbers.

The information will be:

- All that is on automated systems
- Most paper based information
- Included in Emails
- Information kept in paper filing systems
- Information that was intended to be automated, e.g. notes taken at meetings.

4. The process – handling Subject Access Requests

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 responding to an SAR you need to be able to decide what information we hold is personal data and, if so, whose personal data it is.

The Data Protection Act 1988 (DPA) provides that for information to be personal data, it must relate to a living individual to be identified from that information (either on its own or in conjunction with other information likely to come into the organisation possession).

4.1. Disclosure of Information

Every case should be considered on a case by case basis and where possible every effort should be taken to adhere to the guidelines below.

- The SAR should be completed and presented as soon as possible within 40 calendar days of receiving the written request, proof of ID and the £10 fee.
- An individual making a request may specify that their request is limited to personal data of any prescribed description.
- SARs can sometimes be declined due to the cost of fulfilling the request HBC dedicates up to £450 per request, which amounts to 18 hours of work, regardless of the worker dealing with the Subject Access Request.
- The DPA requires that the data/ information be provided to the individual in an intelligible form for the average person. However, the data/ information does not need to be in an intelligible form for specific individuals, but it is good practice to ensure that the individual is able to understand the information provided.
- If a court believes that HBC has failed to comply with the request in contravention of the provisions below, the court may order complete compliance with the request.

4.2. Relevance

The best way to determine what information should be provided to an individual is to establish why they want the information. If the individual is willing to share the reasons behind their request it will make it easier to acquire the records they want. It would be beneficial to reiterate this throughout the process. The more background information the individual can provide will enable HBC to locate the information promptly and satisfactorily.

4.3. What has to be searched

The DPA does not permit you to exclude information from your response to a SAR merely because it is difficult to access.

- You should be prepared to make extensive efforts to find and retrieve the requested information from all potential records including electronic records, archived information, emails, paper files and/or microfiche records.
- It will always be reasonable and proportionate to search our records and to review the information found with a view to disclosing it.

- It will never be reasonable to deny access to the requested information because responding to the request may be labour-intensive or inconvenient.

4.4. Refusal to Co-operate

If you reasonably require further information in order to satisfactorily identity the individual making a request or to locate the information which they have requested and have informed them of that requirement you are not obliged to comply with their request unless they supply the desired further information.

4.5. Exemptions

There are exemptions to providing an individual with their personal data. These exemptions are detailed in the Data Protection Act 1998, they are:

- Confidential References, e.g. confidential references for jobs;
- Research, history and statistics, e.g. information used as part of an ongoing study, if it is not presently being used to make decisions about an individual;
- Publicly available information, e.g. information already in the public domain that can be sourced elsewhere;
- Crime and taxation, e.g. during a live investigation;
- Management information, e.g. during restructuring or redundancy process;
- Negotiations, e.g. during the negotiation process and the information may change the outcome;
- Legal advice, e.g. If someone had sought legal advice about the individual; and
- Health, social care and education records, e.g. if they may cause harm or create risk.

These exemptions should be adhered to where possible and the onus is on the requester, individual or agency to convince HBC that the requested information is necessary.

4.6. Third Party Information

Responding to a Subject Access Request may lead to incidental disclosure of details relating to a third party.

Third party information should not be disclosed without first seeking the consent of the third party.

In order to determine whether or not it is reasonable to comply with a request without the consent of a third party or other individual concerned, regard should be taken in particular to:

- Any duty of confidentiality owed to the third party;
- The steps taken to seek consent;
- Whether the third party is capable of giving consent; and
- Any express refusal of consent.

If you are unable to obtain consent from the identifiable third party, it is advised that you contact the Constitutional and Administrative Solicitor who will help you to consider/balance the impact of the disclosure or refusal to disclose on the third party and the data subject.

Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However decisions must be made on a case by case basis.

If it is decided that disclosure cannot be made, only that information which could identify the third party should be withheld/ redacted and wherever possible, HBC will follow good practice by explaining to the individual that some information has been withheld and why.

Third parties who regularly supply information should be informed that anything they submit may become available to the data subject through a Subject Access Request.

Workers should be aware that anything written manually or electronically may be requested by a data subject in a Subject Access Request and should exercise caution when discussing clients or service users.

The non disclosure of third party information should not be used as an excuse to refuse an individual information they have requested if the information is not of a sensitive nature and reasonable to disclose.

If you are struggling with an issue of third party disclosure you can consult the Caldicott guidelines but please be aware that the Caldicott guidelines are not law and the DPA, Human Rights Act 1998 and common law will always take precedence. If there is an apparent conflict between legislation and the common law, legislation takes precedence. Any queries contact the Constitutional and Administrative Solicitor.

4.7. Unstructured Personal Data

Unstructured Personal Data is manual information relating to the subject area but does not appear in a personnel file or a file pertaining to the subject area.

HBC is not obliged to provide any unstructured personal data unless the request contains a description of the data.

Even if the requester describes the information in their request, HBC is not obliged to provide unstructured personal data if the estimated cost of complying with the request for unstructured data exceeds the appropriate limit (£450). This exemption only applies if obtaining of the unstructured data, alone, exceeds the appropriate limit.

Any estimate for the purposes of this section must be made in accordance with regulations under the Freedom of Information Act 2000.

5. Retention of Data and Records Management

The maintenance of good record management is crucial to simplifying the Subject Access Request process.

If an individual requests access to historical information you should refer to the HBC Data Protection Policy and Retention of Records Policy, which indicates set timescales for good record keeping.

Information can be accessed from various different locations within HBC and ensuring that you're own records are maintained and accurate is vital. Anything written down, manually or electronically can be used in Subject Access Requests and it is important to note that emails between colleagues can be requested; therefore it is the responsibility of each worker to use common sense when discussing a case or an individual through written communication.

6. Retention of Data and Records Management

The maintenance of good record management is crucial to simplifying the Subject Access Request process.

If an individual requests access to historical information you should refer to the HBC Data Protection Policy and Retention of Records Policy, which indicates set timescales for good record keeping.

Information can be accessed from various different locations within HBC and ensuring that you're own records are maintained and accurate is vital. Anything written down, manually or electronically can be used in Subject Access Requests and it is important to note that emails between colleagues can be requested; therefore it is the responsibility of each worker to use common sense when discussing a case or an individual through written communication.

Subject Access Request Roles and Responsibilities

Subject Access Request Received (via First Contact, Contact Centre, social media etc)

Sent to: the Complaints Officer

Complaints Officer to:

- Request evidence of identity
- Request the fee
- Request additional information to allow the council to identify where the data might be found
- When Third Party request, ensure they are entitled to act on behalf of that individual.

NB
The 40 day timescale commences on receipt of fee and Complaints Officer satisfied on identity.

Allocating the request:

For closed cases in children's services, the following managers will complete SARs on rotation:

Maureen McEnaney
Peter Rigg
Danielle Swainston
Sarah Ward
Jane Young
The new Senior Managers on commencement.

For open cases, or those closed within the previous six months, the relevant Team Manager will complete the request.

For closed cases in adult's services, senior managers will complete SARs on rotation:
Neil Harrison
John Lovatt
Peter Rigg
Sarah Ward

For open cases, or those closed within the previous six months, the relevant Team Manager will complete the request.

The complaints officer will advise the relevant manager on receipt of a request. The officer dealing with the SAR request is known as the **Data Controller (DC).**

The Complaints Officer will:

- Confirm receipt of the SAR (on satisfactory receipt of information confirming identity and fee)
- Confirm the date by which the response will be provided (no later than 40 days).
- Identify case records – these will include:
  - All data relating to the individual held in IT systems
  - Any data in paper files relating to the individual
  - Any other data relating to the individual that they have described
- Document what has been searched and justify any limit placed on the search.
- Work with support officer to ensure that all records are printed
- Work with support officer to identify third party records
- Write to third parties for consent to disclose information
- If unable to obtain third party consent, consult with the Constitutional and Administrative Solicitor to consider/balance the impact of the disclosure or refusal to disclose on the third party and data subject. Consider:
  - Is the information already known to the applicant?
  - Is it confidential or sensitive?
  - What is the relationship between the third party and the applicant?
- Keep the DC informed of third party requests and responses.

The support officer will:

- Sort the Local Authority records in to date order or other order in consultation with the officer completing the disclosure.
- Pass the information to the DC completing the disclosure.

On receipt the DC will:

- Read and review all the information with a view to disclosing it
- Consider each document within the file of information separately
- Redact names of third parties where appropriate
- Explain codes/abbreviations/jargon
- Include information from third parties when appropriate and consent has been given

Before sending the DC will check carefully:

- Has information been redacted properly?
- Can remaining information be disclosed?
- Has a complete (unredacted) setoff records been retained (with a record of what has been redacted)?

Responding:

- Consider offering the opportunity to share the SAR in person.
- Draft your response that should explain whether information has been withheld and why
- Include details of complaints procedure
- If posting, double check that you have the correct address
- Send registered post