Barking & Dagenham

Subject Access Request Policy

If printed, copied, or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

www.lbbd.gov.uk

Document Control

Title	GDPR - Subject Access Request Policy
Document Type	Renewal
Author	Information Governance Manager/DPO
Owner	SIRO
Subject	Information Risk Policy
Government Security Classification	Not Protectively Marked
Created	March 2018
Approved by	Assurance Group
Date Approved	
Review Date	22 May 2020

Version Control

Version	Date	Author	Description of Change
1	01/04/17	Yvonne Mason, Information Governance Manager	New Policy Draft
2	13/05/17	Yvonne Mason, Information Governance Manager	Approved by Assurance Board
3	15/03/18	Yvonne Mason, Information Governance Manager/DPO	Renewal. Amendments to sections 1,2,3,7 and 8
4	02/05/19	Nick Lane	Review
5	22/5/2020	Kim Starbuck, Information Governance Manager/DPO	Review and some minor updates to wording. Point 4 updated to include a request can be 'written or verbal'.
6	31/10.2023	Kim Starbuck, Information Governance Manager/DPO	Review
7	31.03.2025	Kim Starbuck/Rik Mannix (DPO Consultant)	Review

1. Introduction

The GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with six principles (Article 5 of the GDPR):

a) processed lawfully, fairly and in a transparent manner

b) collected and processed for specified, explicit and legitimate purposes and not further processing in a manner that is incompatible with those purposes
c) Adequate, relevant, and limited to what is necessary for the purpose
d) Accurate and kept up to date
e) Not kept for longer than is necessary and subject to appropriate technical and organisation measures to safeguard the rights and freedoms of individuals
f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing; and

Secondly, it provides the following rights for individuals (Articles 13 and 14):

1) Right to be informed
2) Right of access
3) Right to rectification
4) Right to erasure (right to be forgotten)
5) Right to restrict processing
6) Right to data portability
7) Right to object
8) Rights related to automated decision-making including profiling

2. Purpose

This regulation explains the obligations of Data Controllers handling personal data. All staff, including temporary and contract workers, are required to understand and assist Data Subjects when identifying and fulfilling right requests are contractually bound to comply with the Act and other relevant council policies.

This policy defines the internal handling of Data Subject Access Requests (DSARs) received by The Council. The guidance provided ensures such requests are managed in a structured, transparent, and fair manner.

Data protection legislation grants individuals the right to access their personal data held by an organization to verify its lawfulness and accuracy.

3. Scope

This Policy applies to data subjects such as residents, service users and employees who request access to their personal data that is held by the Council. It includes all personal data the Council collects and uses whether it is held in electronic or paper format and includes all structed records including records, voice recordings, photographs and CCTV.

All council employees are responsible for the supporting and handling of DSARs, as requests may be received by any department or individual. Therefore, adherence to this policy is essential.

4. How do you make a subject access request?

A subject access request can be a written or verbal request for personal information (known as personal data) held about you by the council. Generally, you have the right to see what personal information the Council holds about you, you are entitled to be given a description of the information, what we use it for, who we might pass it onto, and any information we might have about the source of the information. However, this right is subject to certain exemptions that are set out in the GDPR.

5. What is personal information?

Personal data is information that relates to a living individual who can be identified either directly, or indirectly from the information. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

- an individual's salary or other financial information
- information about an individual's family life or personal circumstances, employment or personal circumstances, any opinion about an individual's state of mind
- special category personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, genetics, biometrics, physical or mental health, sexual orientation, and membership of a trade union.

6. What is a Data Subject Access Request (DSAR)?

- A DSAR is a request from an individual (the data subject) asking for information regarding the personal data we process concerning them.
- Under data protection legislation:
- Requested information must be provided in a concise, transparent, intelligible, and accessible form using clear and plain language.
- Information must be provided free of charge.
    - A reasonable fee may be charged if a request is manifestly unfounded or excessive, particularly if repetitive.
    - A reasonable fee may also be charged for further copies of the same information, based on administrative costs.

7. Who can make a DSAR?

The following individuals can submit a DSAR:

- The individual themselves.
- A parent/guardian requesting access on behalf of a child.
- A nominated representative (e.g., solicitor or relative) with valid consent from the individual.

DSARs can be submitted via post, email, telephone, or social media.

8. What Information Can Be Requested?

A DSAR entitles individuals to:

- Confirmation of whether personal data is being processed.
- A description of the data, why it is processed, and any third-party recipients.
- A copy of the personal data.
- The source of the data (if available).
- Information about automated decision-making processes that affect them.

9. What do we do when we receive a subject access request?

9.1 Proof of identity

The requestor's identity must be verified before processing a DSAR.

- For personal data requests, authentication can be done using:
- Photographic ID (passport, full UK driving licence).
- Proof of address (recent utility bill, bank statement).

If the requestor is known (e.g., a current or former employee), reasonable checks can confirm identity without additional documents.

For requests concerning another individual, the requestor must provide:

- Signed consent from the data subject.
- Power of Attorney.
- Law enforcement request (See Annex 2).

9.2 If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act on their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 16, we will need to consider whether the child can provide their consent to you acting on their behalf.

Collation of information

9.3 We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information and identify any information provided by a third party or which identifies a third party.

9.4 When responding to a subject access request that involves providing information that relates both to the individual making the request and to another individual we do not have to comply with the request 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

9.5 We may sometimes be able to disclose information relating to a third party and the decision will be on a case-by-case basis. The decision to disclose will be based on balancing the data subject's right of access against the third party's individual rights in respect of their own personal data. If the third-party consents to disclosure then it would be unreasonable not to do so. However, if there is no consent, we will decide whether it is

‘reasonable in all the circumstances’ to disclose the information and will consider the following:-

- Is there any duty of confidentiality owed to the third-party.
- Any steps we have taken to try and obtain third-party consent.
- Whether the third-party is capable of giving consent; and
- Any stated refusal of consent by the third-party.

9.6 Before sharing any information that relates to third parties, we may anonymise information that identifies third parties not already known to the individual and redact (blank out) information that might affect another party’s privacy. We may also summarise information rather than provide a copy of the whole document.

9.6 Issuing our response

6.7 Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at the council.

6.8 We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

8. What is the timeframe for responding to subject access requests?

DSARs must be processed without undue delay and within:

- **One calendar month** from receipt of the request or confirmation of identity (whichever is later).
- **An extension of two months** may be applied for complex requests, with the individual informed within the first month.
- If information cannot be provided, the individual must be informed **within one month** of receipt of the request.

9. Are there any grounds we can rely on for not complying with a subject access request?

Previous request

If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

Exemptions

Some requests may be refused if they are manifestly unfounded, vexatious, repeated, or excessive.

Additionally, certain information is exempt from disclosure under data protection legislation. Possible exemptions would be to safeguard:

- National security
- Defence
- Public security
- The prevention, investigation, detection, or prosecution of criminal offences
- Other important public interests, economic or financial interests, including budgetary and taxation matters, public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- The protection of the individual, or the rights and freedoms of others
- The enforcement of civil law matters.

In such cases, the individual will be informed of:

- The decision and reason for refusal.
- Their right to complain to the supervisory authority.
- Their right to seek a judicial remedy.

If processing a large volume of data, the individual may be asked to specify their request.

Data relating to other individuals' will be removed or redacted unless consent for disclosure is also obtained.

10. Handling DSARS

The DSAR Team oversee DSAR handling, liaising with the Data Protection Officer (DPO) where appropriate. If they are unavailable, responsibility extends to senior management.

Once a DSAR is received, responsible parties will:

- Authenticate the request.
- Investigate, extract, and collate the required information.
-
- Where necessary revert to the Data Subject for further information or clarification. Respond to the request.

For specific data requests (e.g., CCTV, IT, HR), operational responsibility for information extraction lies with relevant departments

10. What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction.

If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

12. Our complaints procedure

If the Data Subject is not satisfied with the Council's response, they can request a review through our internal complaints' procedure, the Information Commissioner or the courts.

The council will deal with any written complaint about the way a request has been handled and about what information has been disclosed.

The Complaints Department can be contacted at:

Complaints and Information Team
Room 218 Barking Town Hall
1 Town Square
Barking
Essex
IG11 7LU

Email: complaints@lbbd.gov.uk

If the Data Subject remain dissatisfied, they have the right to refer the matter to the Information Commissioner.

The Information Commissioner can be contacted at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545 745
Email: enquiries@ico.gsi.gov.uk

13. Policy Review

This policy will be reviewed every 12 months. Policy review will be undertaken by the Information Governance Manager/DPO.