DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

(For employees/workers, elected members and data processors)

Document Ref.	**Data Subject Request Policy & Procedure (Replaces** 'Subject Access Requests Guidance Manual v5)
Version:	**7.2**
Dated:	**31 March 2021**
Document Author:	**IG Team**
Document Owner:	**Information Governance**

Revision History

Version	Date	Revision Author	Summary of Changes
4.0	April 25, 2016	[redacted]	
4.1	May 9, 2016	[redacted]	
5.0	March 22, 2017	[redacted]	
6.0	August 30 , 2018	[redacted]	Replaces 'Subject Access Requests Guidance Manual v5' to include all GDPR Data Subject Rights
6.5	September 25, 2018	[redacted]	Appendix 1 revision: Members' access to personal data
6.6	10 February 2020	[redacted]	Review
7.1	29 April 2021	[redacted]	Annual Review
7.2	27 August 2021	[redacted]	Further review. Amended all references to "GDPR" to "UK GDPR". Amended IG Team role and added CCU role.

Distribution

Name	Position	Date circulated
[redacted]	Head of Information Governance and DPO	July 27, 2018
[redacted]	Director of Residents Experience and Digital	August 31, 2021
Information Risk Board	SIRO, Information Asset Owners and Deputy Information Asset Owners	November 2, 2021

Approval

Name	Position	Sign-off Date
[redacted]	Serious Information Risk Owner	November 30, 2021

CONTENTS

1. INTRODUCTION

This policy is intended to be used when a data subject exercises one or more of the rights they are granted under the 2018 Data Protection Act (the 'DPA') and Article 15 UK GDPR via a request (a 'Data Subject Access Request') to the Council.

This document is primarily aimed at providing additional guidance to Information Asset Owners (IAO), Deputy Information Asset Owners (DIAO) and Data Owners (DO) and explaining how Data Subject Requests should be handled. It should also be used as a reference document for all staff who may be required to assist in handling requests for personal data.

This policy should be considered in conjunction with the following related documents where applicable:

Data Protection Policy

Information Protection and Handling Policy

Information Management Policy

Redaction Guidance of SARs

These documents can be found on the Information Governance SharePoint page (link below)

https://lambeth.sharepoint.com/sites/InformationGovernanceNewVersion

1.1 DEFINITIONS

'Controller' (Lambeth Council) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'Data Protection Act 2018 (DPA)' The DPA is UK legislation that is required to ensure the effective operation of the UK GDPR in the UK. It supersedes the DPA 1998. Importantly, it contains the various exceptions to Subject access rights that apply in the UK.

'Data Protection Officer' The DPO is responsible for monitoring internal compliance, advising on data protection obligations and compliance, reviewing Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and the supervisory authority (Information Commissioner's Office).

'General Data Protection Regulation (GDPR)' the General Data Protection Regulation (GDPR): European legislation which came into force in May 2018. It applies directly in the UK and post Brexit is known the UK GDPR. It contains the fundamental principles, rights, and obligations in relation to data protection.

‘**Personal Data Breach**’ means a breach of security, an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

‘**Process’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

‘**Processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘**Processing**’ refers to the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

‘**Personal Data**’ means any information relating to an **identifiable living natural person** (also known as the ‘**data subject**’);

> ‘**A living identifiable natural person**’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘Special categories of personal data’ as defined in Article 9(1) GDPR, special category data is more sensitive, and so needs more protection. Therefore, to process these, there are extra conditions for processing.

Special category data is any data relating to the Data Subject’s:

- race or ethnic origin;
- his/her political opinions or trade union membership;
- his/her religious beliefs;
- his/her physical or mental health or condition;
- his/her sex life or sexual orientation.
- genetic and biometric data

‘Subject Access Request’ (referred to as a ‘SAR’) is a request made by or on behalf of an individual for the information held by the data controller which he or she is entitled to ask for under the DPA’s and Article 15 UK GDPR ‘Right of Access’.

‘Subject Request’ is a request made by or on behalf of an individual to exercise **any of the ‘Rights of the Data Subject’** under the DPA and UK GDPR (see table of contents for a list of rights).

'**Supervisory Authority**' is the ICO (The Information Commissioner's Office) as far as Lambeth Council's processing activities are concerned

1.2 GENERAL POINTS

The following general points apply to all requests described in this document and are based on Article 12 of the UK GDPR:

1. Information shall be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.
2. Information may be provided in writing, or electronically. If the individual submitted the SAR electronically (eg by email or via social media), you must provide a copy in a commonly used electronic format. You may choose the format, unless the requester makes a reasonable request for you to provide it in another commonly used format (electronic or otherwise).
3. If the individual submitted the SAR by other means (eg by letter or verbally), you can provide a copy in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for you to provide it in another commonly used format. However, where the information is sensitive, you should ensure that you transfer it to the requester using an appropriately secure method
4. The data subject may verbally request their personal information (e.g. over the telephone or face to face), as long as the identity of the data subject has been established.
5. We must promptly act on a request from a data subject, unless we are unable to validate their identity.
6. We must **provide information** without undue delay and **within a maximum of one month** from the receipt of the request (or proof of identity).
7. The response **timescale may be extended by up to two further months** for complex or a high volume of requests – the **data subject must be informed of this as soon as possible within one month of the request, and the reasons for the delay given**.
8. If a request is made via electronic form, the response should be via electronic means where possible, unless the data subject requests otherwise.
9. If it is decided that we will not comply with a request, **we must inform the data subject without delay and at the latest within a month**, stating the reason(s) and informing the data subject of their right to complain to the supervisory authority (the ICO).
10. Generally, responses to requests will be made **free of charge**, **unless they are "manifestly unfounded or excessive"**, in which case we will either charge a reasonable fee or refuse to action the request.
11. If there is doubt about a data subject's identity, we may request further information to establish it.

1.2.1 What is a valid Subject Request?

1. A valid request:

   a) Must be for/regarding personal data.
   b) May be made orally (over the telephone or face to face) or in a permanent form (in writing, email).
   c) Must contain sufficient information to verify the identity of the person making the request and to locate the information which that person seeks.

2. The request does not have to cite the legislation, nor explain the reasons why the request is being made.

3. Where an individual may be unable to make a written request without support or because English is not the person's first language then we should provide reasonable assistance to the individual. For example the member of staff may record the request for the applicant, then send the completed request form to them with a covering note asking for the ID if necessary. Should the applicant wish to proceed with the request they should send the request form back together with a copy of the ID.

1.2.2 Who can make a request under the Act?

Any living individual has a right to request access to the personal data that the Council holds on them. A resident of Lambeth, a Council employee, or any other person that the Council holds personal data for will therefore have a right to request access to their personal data.

1.2.3 Making a request on behalf of another person

1. A data subject may provide a form of authority to another person, for example a relative, to make a subject request on their behalf. Written authority from the data subject should be provided before the Council can proceed with a request from an agent. The Council will also require ID from both individuals and must be satisfied the data subject has authorised the disclosure to the third party.

2. In the case of a member acting on behalf of their constituent (who is the data subject), it can be assumed that they are authorised to make the request without requiring further clarification (see Appendix 1).

3. A child is, in theory, entitled to a make a subject access request. However, a request from a child should only be complied with if it is thought they understand the nature of the request. As a general rule, a child aged 12 or over is presumed to be of sufficient age and maturity to be able to make a request for their own data. Where a child is deemed able to make a subject access request, the officer handling the request should reply directly to the child (you may, however, allow the parent to exercise the child's rights on their behalf if the child authorizes this, or if it is evident that this is in the best interests of the child).

4. If the child is not of sufficient age and maturity, then a person with parental responsibility is entitled to make a request on their behalf. We will ask for evidence of the parental responsibility (can usually be found on the birth certificate). The officer should be satisfied that the person with parental responsibility is acting in the best interests of the child before releasing the data. Caution should be exercised where child custody or abuse cases are concerned and where the child has given information to a practitioner on an expectation of confidentiality.

5. If the nature of the request suggests that the data subject is/or has been involved with Children and Young Peoples' Service (CYPS) or Adult and Community Services (ACS) then the Officer dealing with the request should check with the relevant department to

establish if the data subject has the necessary mental capacity to be able to authorise another individual to access their data.

6. An agent appointed by the Court of Protection or with a valid Power of Attorney may make a request on behalf of a mentally incapacitated individual. Upon receipt of such a request, the officer should check the validity of the Power of Attorney or the Court of Protection Order. A Power of Attorney must specify the purposes it is granted for and it must be a certified copy (i.e. the document has the original stamp and signature of a solicitor).

7. We must ensure we take care where we receive requests from spouses, partners or other relatives who may claim to be authorised to access the data – unauthorised disclosures to family members are a frequent cause of complaint to the Information Commissioner.

8. If you doubt the agent’s authority, seek advice from the Council’s IG team

1.2.4 What about rights of access to information relating to deceased individuals?

1. The DPA only applies to the personal data of living individuals and as such does not give rights of access to deceased individuals’ data.

2. Whilst the DPA does not apply to deceased individuals’ information, the Council does still owe a common law duty of confidentiality to the deceased person’s estate and advice should be sought before disclosing information relating to deceased individuals

3. Therefore a personal representative or executor can access information to benefit the deceased's estate, as can an individual who was a dependent of the deceased and who has a claim relating to that dependency which has arisen from the death.

4. If you receive a request for access to information relating to a deceased individual contact the Council's IG team for further advice (Appendix 1).

1.2.5 What is an individual entitled to following a subject access request?

1. Upon making a request and providing proof of identity to the Council, the individual is entitled to obtain the following information:

    a. Confirmation that the Council is processing their personal data;
    b. A copy of their personal data; and
    c. Other supplementary information – corresponding to the information that should be provided in a privacy notice (i.e. purposes of processing, categories of personal data, who the personal data is shared with, retention period for storing the personal data, existence of rights to rectification, erasure, restriction, to object to such processing or to automated decision-making/profiling, to lodge a complaint with the ICO, and the source of data if not obtained from the individual);

2. The individual is also entitled to a copy of the manual and computerised personal data the Council holds on them (unless an exemption applies). The personal data should also be provided in an intelligible form.

3. The entitlement is to receive personal data, not documents. As such an individual is not necessarily entitled to the original documents and all the information that they contain. However, providing copies of the documents that contain personal data is often the simplest and most cost-effective way of dealing with a subject access request.

1.2.6 Does the DPA give an individual the right to view their personal data?

1. Individuals may request, or even demand, to view their file. The DPA does not provide individuals with this right. The Act only entitles them to copies of their personal data, for example via the provision of photocopied documents containing personal data. However, the Act provides that the Council can fulfil its obligations under the subject access provisions by allowing an individual to view their records (rather than being provided with a copy), providing that the individual agrees to this proposal.

2. In the case of requests for social work records it may be prudent to invite the individual into the Council to view their records, with a social worker available to help the applicant understand and "take in" the information that is held on them.

3. If an individual agrees to a viewing of their records and they have specific needs in

relation to language or disability, arrangements must be made to present the information in a suitable manner and to involve approved interpreters. Consideration should also be given as to the accessibility of the building where the viewing is to take place.

4. Interpretative and supportive counselling may be advisable in certain cases, using a number of interviews to disclose the information if the person is willing to proceed in this manner.

The public can get more information on making a subject access request to the Council here

1.3 ROLES AND RESPONSIBILITIES

Deputy Information Asset Owner (DIAO) within each directorate

- Identify who is best placed in their directorate area to respond to the SAR request.
- Act as the point of contact for their directorate area.
- Monitor requests allocated to their directorate area, and follow-up where cases are becoming due.
- Notify the FOI Coordinator immediately if there is any part of the request that cannot be answered within their directorate area.
- Notify the FOI Coordinator within 5 working days if further clarification of the request is needed.
- Notify the FOI Coordinator within 5 working days if they are concerned about releasing the information.
- Raising awareness of Data Subject Request rights within the business areas.
- Notifying the FOI Coordinator of changes to their directorate area of responsibility and ensuring an adequate handover of duties to a replacement officer if leaving post.
- Escalate and deal with internal reviews.

Call Centre (Capita)

- Logs Requests and allocates coordinated requests to Deputy Information Asset Owners (DIAO), referring to the Council’s Knowledge Base, within service areas giving due dates for response.

Corporate Complaints Unit (CCU)

- Maintains and updates the Council’s Knowledge Base document.

- Administers the ***iCasework*** system

Information Governance Team (IG Team)

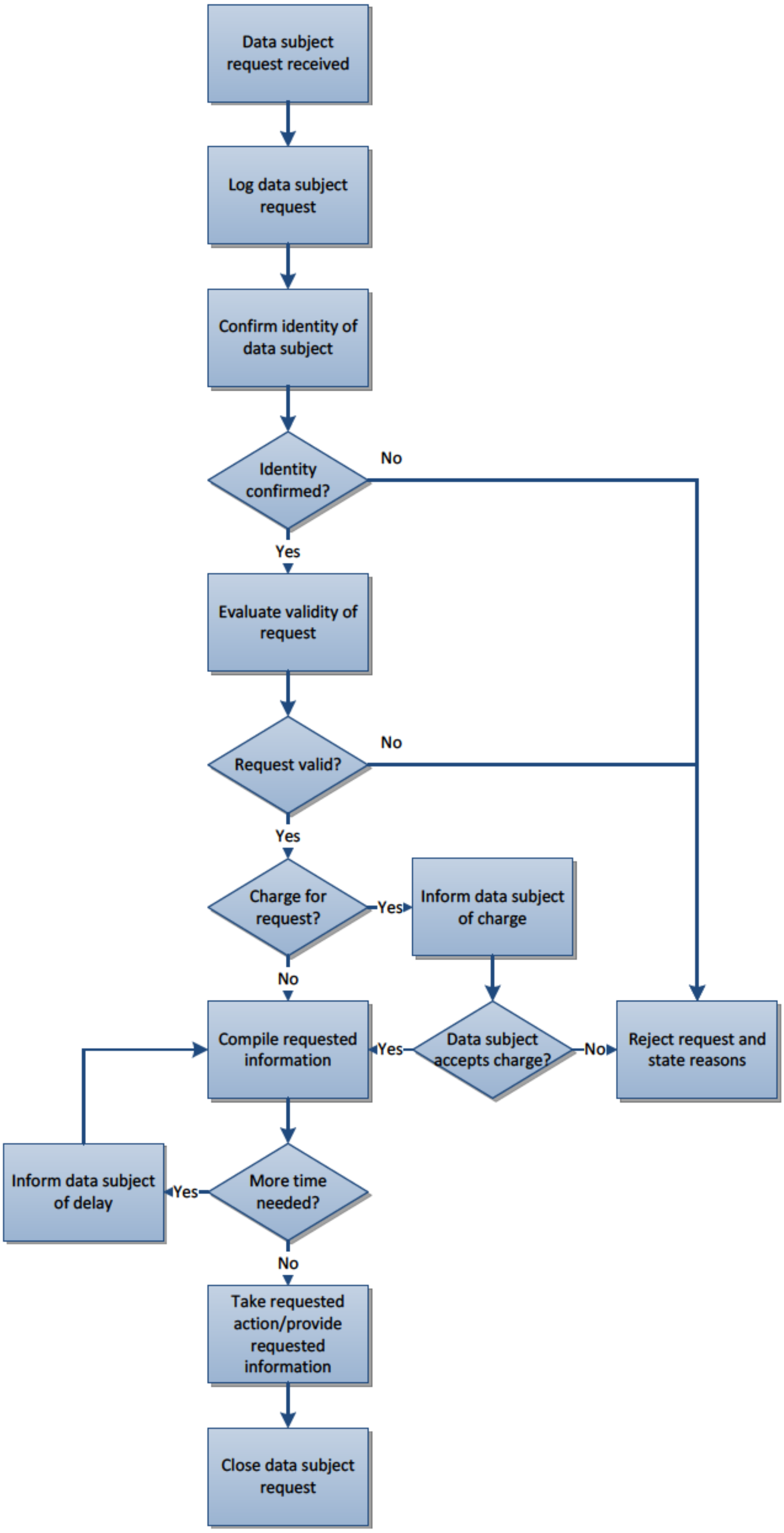
- Head of Information Governance will carry out the DPO role.

- Provides advice and assistance for the DIAO on conducting of SAR internal reviews, exemptions, non-disclosure of information.

- Act as the main point of contact with the Information Commissioner's Office (ICO).

2. SUBJECT REQUEST PROCEDURE

2.1 REQUEST PROCEDURE FLOWCHART



2.2 Handling a Subject Access Request

1. Subject Access Requests (SARs) can be received by any member of staff within the Council.

2. All staff need to be able to recognise a subject request, know who to go to for advice and guidance, and what to do with a request.

3. Any correspondence received by a member of staff asking to access personal data should be sent immediately to dataprotection@lambeth.gov.uk.

4. Staff must be aware a request can be made verbally. Staff receiving a request verbal request should encourage the requestor to send a written request. Staff should ensure that verbal subject access requests are recorded and acted upon. Staff receiving a verbal request can themselves send full details of the request and the requestor to dataprotection@lambeth.gov.uk.

2.3 Receipt, Logging and Assignment of the Subject Request

1. When opening and sorting the post, Subject Access Request letters or data protection enquiries should be scanned to the Corporate Complaints Team on Omnidox or scanned by Canon in Winchester to electronic mail and sent to dataprotection@lambeth.gov.uk.

2. Subject access requests must be scanned and sent to the contact centre to be logged onto ***iCasework*** immediately and no later than 48 hours of receipt to email: dataprotection@lambeth.gov.uk

3. Once the request is validly made (including verification of ID) it will be assigned through ***iCasework*** directly to the designated person from the Knowledgebase. If the request includes information held by another Directorate, the designated case officer leads on subject requests retrieving the data within the service area to handle.

4. Where the SAR crosses across several Directorate areas of responsibility the area who handles majority of the request will take the lead. The CCU Team will provide support to the lead case officer. All Directorates are required to provide assistance to the lead case officer as reasonably requested.

5. Requests for Electoral Registration data should be logged and passed directly to the Electoral Registration Officer and requests for Births, Marriages and Deaths should be logged and directly passed to the Births, Marriages Death Registration officer as these officers are Data Controllers in their own right. Requests under the UK GDPR and the Data Protection Act should be directly passed to them to respond to unless there is any other part of the request which falls to another part of the Council to answer in which case they should be assigned to the IG Team who will coordinate a response.

2.4 Validation, Clarification and Classification

2.4.1 After the subject access request is logged and allocated to the appropriate service area, in the majority of case via the Call Centre, the responsible DIAO is responsible for ensuring that sufficient checks to authenticate that the request is valid (i.e. a clear request for information held, proof of identity, proof of address, etc.) by following these general steps:

- Clarify information sought and type of request
- Validate the identity of the individual
- Classify the request (by Data Subject Right):
    i. Withdrawal of Consent
    ii. Access (including CCTV)
    iii. Rectification
    iv. Erasure
    v. Restriction of Processing
    vi. Objection to Processing
    vii. Data Portability
    viii. Automated-decision making/profiling

- Assess whether request is ‘manifestly unfounded or excessive’ (charge fee/refuse request, check with Information Governance if/when unsure).
- Inform and explain data subject of reason for ‘manifestly unfounded or excessive’ fee (if applicable, i.e. too many requests in a short period).
- Search for all records that contain information where the focus is about the individual
- Assess the content of the records
- Rectify/erase personal data and/or restrict processing (if applicable)
- Redact or exempt specific personal data (if applicable)
- Send response to individual (e.g. confirming or denying the specific request, as applicable) and **log as closed (with Call Centre) within one month of request, identity validation or collection of ‘manifestly unfounded or excessive’ fee** (it is possible to extend by further two months if the request is complex but you must let the individual know as soon as possible and no later than within one month of receiving the request and explain why the extension is necessary).

2.4.2 Clarifying the request

1. The Council may seek further information from the applicant where this is reasonably required in order to be able to locate the information that the applicant is seeking access to.

2. Generally Subject Access Requests for ‘all personal data’ are valid, and the service area DIAO should not simply ask the applicant to be more specific if the location of the data is already known. If clarity is sought please bear in mind that the applicant will not be aware of the different ways in which the Council holds their personal data.

2.4.3 Verification of the identity of the individual

1. The Council itself must be satisfied as to the identity of the individual making the request by asking the individual to produce a copy of a document that might reasonably be expected to be only in their possession (e.g. their passport, driving licence).

2. If the request is from an agent of the data subject; check that they have the necessary authority. This is known as a Letter of Authority and typically will be a signed and dated letter from the individual whose data is being requested confirming that they are happy for the agent to act on their behalf.

3. There is no need to verify where already in an established relationship with the data

subject, for example a request comes from an employee Lambeth mail address.

2.4.4 Fee charging

1. The UK GDPR and DPA has abolished the standard fee for Subject Requests. Only if you consider that a request is manifestly unfounded or excessive may you either request a ‘reasonable fee’ to deal with the request or refuse the request (for all questions or inquiries regarding fees, contact Lambeth Council’s Data Protection Officer). You must explain your decision to the requested and inform them of the right to make a complaint to the ICO.

2. If a fee is required, it will be based on the administrative costs of complying with the request. If the Council decides to charge a fee contact the individual must be contacted promptly and informed of the decision and the fee. The Council does need to comply with the request until you have received the fee.

2.5 Who deals with a subject request?

1. Responses to requests should be coordinated by the relevant directorate area DIAO.

2. Requests for access to personal data held by a number of different departments across the Council should be directed via Corporate Complaints Team to the directorate DIAO where most of the personal data is likely held.

2.6 Time limits

1. The statutory time limit for complying with a subject request is one calendar month. The month will normally start from the date the Council receives the request. However, if one or more of the items listed in (a) – (e) below have not been provided, the time limit will not commence until that item has been provided:

    a. Information reasonably required to validate the identity of the data subject.
    b. Information reasonably required to locate the personal data requested.
    c. Written authority from the data subject where there is a third-party person applying on their behalf of the data subject.
    d. A certified power of attorney or court of protection order (where applicable).
    e. Collection of ‘manifestly unfounded or excessive’ fee (where applicable).

2. If the request does not meet the criteria identified in (a) to (e) send a letter to the applicant/their agent requesting the necessary fee/information. Any further information/fee required should be asked for promptly within 7 calendar days.

3. One of the main reasons why people complain to the Information Commissioner is because their subject request was not completed within the statutory time limit.

4. Every effort should be made to comply with the time limit. If it is clear the request and/or data collection and provision is going to exceed this limit, then the applicant should be advised within one month of the date when their personal data is likely to be provided, not to exceed two additional months.

5. If we do not receive a response within 30 days to the letter asking for the further information required, then we are not obliged to deal with the request and shall record the reason(s) accordingly on iCasework.

2.7 Searching for records / Types of Records

When searching for records in order to respond to a subject request you should bear in mind that your directorate may not be the only directorate which has dealt with the individual concerned. Checks should be made with other departments/teams, such as the Corporate Complaints Team, to capture any additional records that they hold.

2.7.1 Record types

a. Manual files

1. The type of manual files held on the data subject will depend on the nature of their involvement with the Council. The computerized information held on an individual may well indicate if manual personal data is held.

2. Some manual files may be stored off site. It is important to confirm whether this is the case and ensure that these files are located so that access can be given.

b. Computerised personal data

Below is a non-exhaustive list of the databases that hold personal data:

1. **Framework** is the database used by ACS and CYPS to record details in respect of social work clients. This database contains personal information, such as, assessments carried out on clients, correspondence with clients and other third parties involved in the care of that individual.
2. **Academy** is used to record case details in respect of Council Tax, Housing Benefit and Council Tax Benefit.
3. **Anite** is an electronic document records management solution which holds correspondence relating to Housing, Housing Benefit, Council Tax, Council Tax Benefit and ACS matters.
4. **HICS/SAFFRON/Northgate(SX3)** contain tenancy case details, repairs information on Council properties and housing register details.
5. **Uniform** contains information relating to environmental complaints (inc noise complaints), environment health and licensing, land charges, planning applications, private sector housing and building control data.
6. **ICPS** contain details of Penalty Charge Notices issued and related correspondence.
7. **i-Casework (previously held in RESPOND for requests made before May 2013)** is the Council's Corporate Complaints database which contains correspondence and activity notes on complaints, FOIs, MEs and SARs that individuals have made to the Council.
8. **Oracle HRIS** contains personal details in respect of employees of the Council.
9. **CRM (oneserve)** holds the basic contact details (i.e. name and address) of individuals who have contacted Lambeth Service Centre on a particular matter. The CRM also shows which Council departments that individual has had interactions with.
10. **Impulse** contains case details relating to school admissions and appeals.
11. **YOIS** is the database used by the Youth Offending Team and contains case details and activity logs on their clients.
12. **SENATE** is the Special Educational Needs database that contains case details of customers who have had assessments.
13. **EPIC** is the database used by the Educational Psychologists it contains case details of client who have been referred for assessments.

Our **Archive** which can be accessed provided by Restore. You will need to register. The link to Records Management and Archiving is set out below.

Link to Records Management and Archiving

1. We are also obliged to handle requests for personal data held within e-mails. The Information Commissioner has developed guidance in this area as e-mail systems are often difficult to search. This guidance provides that it may be advisable to ask the data subject for additional information to help narrow down the search, and that the following should be taken into consideration:

    a. Whether the data subject indicates that any data might be held in e-mails.
    b. Whether the data subject can supply the authors and recipients of the emails.
    c. Whether the data subject can indicate the subject of the e-mails.
    d. Whether staff who have had dealings with the data subject are aware of emails exchanged either internally or externally relating to the data subject.

2. In the first instance, the FOI Coordinator should contact those individuals who have had dealings with the data subject to see if there are any relevant e-mails in their Outlook account (this is particularly relevant to requests from employees and former Council employees). E-mails containing personal data relating to the data subject should be copied and forwarded to the service area's DIAO or designated case officer. Further information should only be sought from the data subject where it is reasonably required in order to locate data they are seeking access to.

    NB: it is a criminal offence for an individual to alter, block or destroy information, where their intention is to prevent the disclosure of the information to the data subject.

c. Back-up data

1. Back-up data may have to be supplied if requested, though only if it contains information not held on (or different to) the live system. This may be extremely time consuming and costly.

2. The Council's policy generally is to determine whether we would be prepared to retrieve the data for our own purposes. If we would, then we ought to do the same for a data subject. The service area's DIAO should contact the DPO if they receive a request for back-up data.

d. CCTV

Click link to go to documents to request CCTV SAR Link to requests of SARs / CCTV

1. Where the Council uses CCTV cameras the images that they capture may need to be provided in response to a subject access request, for example Streetcare or Parking Control.

2. It is not necessary to check and supply footage unless the individual has specifically requested it. When asking for this type of data the individual will need to

complete the Council's CCTV SAR request form to help us to find the images (available http://www.lambeth.gov.uk/parking-transport- and-streets/parking-fines/get-a-copy-of-cctv-footage). The following information will be needed: date and place of the incident, approximate time, description of the individual, for example what they were wearing, and any other information which may help identify the images requested.

3. If a request for CCTV footage is received and that information would normally be destroyed within the month for compliance, then the footage must not be deleted until the data has been provided. Once you have given the individual a copy of the footage. You should confirm that the data has been/ or is about to be deleted when providing your response. However, staff must not delete the recording solely on the basis that they want to prevent the data subject from gaining access, as this is a criminal offence.

e. Recorded telephone calls

1. The data subject may request access to the personal data contained within a telephone recording. This data can be provided in the form of a recording of the telephone conversation, or alternatively, through the provision of a transcript.

2. If the deletion date for the telephone recording occurs within the time period for compliance with the request (1 month), then the recording should not be deleted. Once you have given the individual a copy of it. You should confirm that the data has been/or is about to be deleted when providing your response. However, staff must not delete the recording solely on the basis that they want to prevent the data subject from gaining access, as this is a criminal offence.

3. Non-automated calls received by the Lambeth Service Centre are recorded and are normally held for a period of 6 months.

f. Personal data held within unstructured manual records

1. From 1 January 2005 individuals have had a right to request access to their personal data which is contained within unstructured manual records (i.e. a manual file not held by reference to the individual).

2. If an individual is requesting access to personal data which is held within an unstructured record, they will need to specify the information that they are seeking so that we can locate it (e.g. "I am requesting access to the personal data held about me which is contained in the minutes of your meeting of 5th June 2021").

g. Integrated social care and health records

1. Where an applicant is seeking access to the joint health and social care record, they should not be required to apply to both the Local Authority and the NHS Trust. In these circumstances the Officer handling the request must liaise with the NHS Trust.

2.8 Assessing the contents of a record (including third party details)

1. Once all the personal data requested has been located, the service area's DIAO should assess the content of the records for:

a. Third party data.
b. Unintelligible terms.
c. Personal data that is covered by one of the DPA's exemptions.

2. This section only deals with issues regarding third party data and unintelligible terms. Guidance on the Act's exemptions is contained in section 3.3.

3. If the information held is inaccurate then amendments should not be made before the data is sent to the individual. The individual should be informed that we are aware of the inaccuracy and have taken steps to amend or annotate the original data.

2.9 Third party information

1. The DPA acknowledges a third party's right to privacy where they can be identified from another individual's personal data (e.g. a complaint letter from a member of public held within another individual's housing file). The UK GDPR and DPA introduce a number of criteria which aim to balance an individual's right of access against a third party's right to privacy.

   Personal data which also identifies a third party could be withheld unless:
   a. The third party has consented to the disclosure.
   b. It is reasonable in all the circumstances (see below) to comply with the request without their consent.
   c. The third party identifiers can be removed from the document and the data subject can still receive the personal data contained within that document. In practice this may be difficult as the subject matter of the information may mean that the data subject is still able to infer the identity of the third party.

2. When deciding whether it is reasonable to disclose without consent, the following should be considered:

a. Any duty of confidentiality owed to the third party (i.e. consider the nature of the data and if the third party provided this information to the Council on an understanding of confidentiality).
b. Any steps taken to obtain the third party's consent.
c. Whether the third party is capable of giving consent.
d. Any express refusal of consent by the third party and the reason for the refusal.

3. If the third party has not consented, this does not mean that personal data should be automatically withheld. Their reason for the refusal should be sought, as these reasons will determine whether it is reasonable in all the circumstances to withhold information that identifies them. For example, it may be reasonable to withhold data where the third party justifiably believes that disclosure may lead to physical retribution by the data subject. However, it may not be reasonable to withhold an individual's name if they have been acting in a work capacity and the documents show inability or incompetence in work which they are accountable for.

4. If the service area's DIAO decides that the data identifying the third party should not be provided, only that information which identifies the third party (either explicitly in the document or as the source of the information) may be withheld. This may require documents to be edited, either by blocking out third party identifiers or by retyping the information with third party details omitted. Please refer to the Lambeth SARs Redaction guidance.

2.10 Providing information in an intelligible form

a. Data subjects are entitled to be provided with a copy of their personal data in an intelligible form, with any codes, abbreviations or technical terms explained (e.g. HICS printouts contain a number of codes and abbreviations).

b. This also means that if the requestor is a child or someone who lacks the mental capacity, then the information may need to be explained in simpler terms than when dealing with an adult.

c. We should always communicate with members of the public using plain English at all times. You should avoid using acronyms or jargon that only we would be familiar with.

2.11 Inaccurate or expired information

Should you note whilst collating a SAR that information on a file is inaccurate; you CANNOT simply amend the data and then send it out.

Similarly, should you note whilst collating a SAR that information on a file should have previously been deleted / disposed of you CANNOT simply destroy it.

Please be aware that it is a criminal offence to alter or destroy data once it has been requested under subject access, an appropriate process must be followed.

The correct process is:

- Where data is shown to be inaccurate the data must still be provided in its current state, provided you don't disclose another person's data as a result, or another exemption applies. In addition, a note should be provided to the requester apologising for the error in the data, stating that the information was inaccurate but has now been amended. A revised copy can then be provided and the inaccurate data amended on file.

- Where the data has been retained for longer than is appropriate. You must still provide a copy of the data, but state that it should not have been retained and advise that it has now been removed from the file and safely destroyed.

- The Data Protection Act requires organisations to retain accurate and up to date records. If you notice that information is repeatedly inaccurate or is not being disposed of in a timely manner, this must be raised with your manager as a risk and team practices should be amended to ensure the issue is appropriately addressed.

2.12 Dispatch and Completion

Always observe all policies within the Information Governance Management Framework, specifically the Information Protection and Handling policy and Redaction Guidance together the Information Security Policy when sending out information, ensuring at all times information is sent securely electronically via Egress if electronic and marked appropriately or by special delivery if manually held.

2.12.1 Dispatch

1. Before sending the data, check:

    a. Whether the consent of any relevant third party has been obtained.
    b. If not, whether the data has been edited to conceal the third party's identity, or
    c. Whether it is reasonable to disclose the data without consent.
    d. If the third party is a Council employee acting in that capacity, it should be noted that employee names are already routinely disclosed. However, officers may delete names of staff where it is considered appropriate in the circumstances to do so (e.g. where this may put that employee in danger).
    e. Double accuracy check the data subject's email or address is correct

2. Ensure explanations of all abbreviations and codes have been provided, where relevant.

3. Copy the edited manual and computer data and, if there is a considerable amount of data, compile a schedule of all documents to be disclosed.

4. Make a note on the relevant file of any information/documents that have not been provided in response to the request, stating the reason for the nondisclosure (e.g. third party data or the particular exemption that applies). This information will be of assistance if we receive a subsequent request or if we have to justify our decision to the Information Commissioner.

5. Send the requested copies with a covering letter (***iCasework*** contains a template letter that can be adapted where necessary) to the applicant via Egress, advising them:

    a. That any query about the response should be addressed to the relevant directorate DIAO.
    b. If any exemptions that have been relied on if withholding information (unless the disclosure of the particular exemption would cause prejudice, for example to a criminal investigation).
    c. That if they are dissatisfied with the way their subject access request has been dealt with, they can seek an internal review by the directorate.
    d. If the data subject remains dissatisfied with the internal review response the requester can refer to the Information Commissioner to undertake an assessment (a copy of the internal review procedure is contained within Appendix 4).

2.12.2 Completion and Logging the request as dealt with

1. Record on ***i-Casework*** the date that the request has been complied with and closed. Note the amount of time spent dealing with the request.

2. Include on the tracking database the letter(s) sent from the data subject/their agent, together with a copy of the letter(s) sent in response to the request and a schedule of the personal data provided.

There are some notable exceptions to the standard approach. These are:

Is the information personal data?
Yes

Is the information parentage data – Request under Adoption Agencies Regulations 1983 or Adopted Persons (Birth Records) Regulations 1991

Is the information pension data – Request under Occupational Pension Schemes (Disclosure Information) Regulations 1996 or Stakeholder Pension Schemes Regulations 2000)

Is the information industrial data – Request under Trade Union and Labour Relations (Consolidation) Act 1992, Transfer of Undertakings (Protection of Employment) regulations 1991; Health & Safety at Work Act 1974, Transnational Information and Consultation of Employees Regulations 1989 or Information and Consultation of Employees Regulations 2004

Is the information wages data – Request under National Minimum Wage Act 1998

Is the information Criminal records data – Request/ obtain access under Police and Crime Act 2017

<u>Publicly available information</u>

Where an organisation is obliged by or under an enactment to make information available to the public, personal data that is included in that information is exempt from subject access provisions. For example, details of individuals making a planning application, HMO Licence, or Parking Ticket Appeals.

The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about the individuals, the additional data is not exempt (i.e. must be considered for disclosure under subject access) even if the organisation publishes that data.

3. EXEMPTIONS TO THE RIGHT OF ACCESS

3.1 Exemptions

A summary of some of the more commonly used exemptions from the right of subject access, and of the restrictions (similar to exemptions) built into the DPA is produced at Appendix 5 of this policy.

The Council is not obliged to grant subject access if either an exemption or a restriction applies. However, you must consider each exemption or restriction on a case-by-case basis, as they only allow you to withhold information to the *minimum extent necessary*.

The Council therefore cannot necessarily apply an exemption to a whole file. Each exemption must be placed on a document or paragraph of information as opposed to a blanket exemption for one file or matter.

If you withhold personal data from an applicant you **must** make a file note of:

(i) the information withheld,
(ii) the exemption or restriction relied upon for each piece of withheld information, and
(iii) the reasons why the exemption or restriction applies.

There is no requirement under the Act to tell the requester that an exemption has been applied. However, the ICO Code of Practice states that best practice would be to state in your response (to the extent it can) what information has been withheld and the reasons why.

1. There are limited exemptions to the right of subject access which allow information to be withheld from an applicant. However, they should be approached with caution, and applied on a case-by-case basis.

2. This section will only cover those exemptions that may apply to the Council. In complex cases seek advice from the Council's FOI Co-ordinator before withholding (or disclosing) information.

There is no exemption that applies to disclosure of embarrassing comments.

3.2 Disproportionate effort

1. This exemption has a limited effect as it only relates to the effort of providing a permanent copy of the information. The Council may still be required to allow the individual access to view their personal data if a copy cannot be provided. However, allowing a viewing could be problematic as there may be exempt information in the computerised/manual records. Advice should be sought from the Data Protection Officer prior to relying on this exemption.

2. The term "manifestly unfounded or excessive" is not defined in the Act, so it is a question of fact in each case. The following may be taken into consideration:

   a. The cost of providing the information.
   b. The length of time it may take to provide the information.
   c. How difficult it may be for information to be provided.

3. These issues must be balanced against the effect that withholding the information would have on the individual. The greater the adverse effect, the less likely the exemption could be applied.

3.3 Repeated requests

1. There is no requirement to comply with a request from an individual which is identical or similar to a previous request from them, unless a "reasonable interval" has elapsed.

2. Factors to consider when deciding what amounts to a "reasonable interval" are:

   a. The nature of the data.
   b. The purposes for which the data are processed.
   c. The frequency with which the data are altered.

3. Caution should be exercised here as the individual may have only requested specific personal data in their original request, and their subsequent request could be for other personal data held.

3.4 Crime and taxation

Personal data is exempt from subject access where disclosure would be likely to prejudice:

i. the prevention or detection of crime
ii. the apprehension or prosecution of offenders, or
iii. the assessment or collection of any tax or duty.

This is not a blanket exemption: you must show *in each particular case* why disclosure would be likely to prejudice one or more of these purposes.

The exemption also extends to risk assessments of non-payment, non-compliance or fraud in relation to taxes or duties

1. The DPA allows information which is processed for investigating a potential criminal offence to be withheld following a subject access request if, by disclosing the information, an investigation would be significantly prejudiced. This is likely to apply if we are prosecuting individuals who may have committed an offence or where we are working closely with the Police or other prosecuting body in respect of an individual.

2. Similar, information which is processed in connection with the assessment or collection of any tax may be withheld following a subject access request if, by disclosing the information, that assessment or collection would be significantly prejudiced.

3. Decisions on the withholding of personal data should be made on a case-by-case basis. Whoever is involved in the investigation should be consulted when the request is received.

4. The Information Commissioner's view is that there must be "a substantial chance rather than a mere risk that in a particular case the purposes (i.e. the investigation or assessment / collection) would be noticeably damaged". Therefore, information held by the Council should only be withheld where it can be shown beyond doubt that current or future processing carried out by the Council (or other prosecuting body) would be prejudiced by such a disclosure.

5. Where redactions are made they should only affect the prejudicial information. Other information which would not prejudice an investigation should therefore be disclosed as normal in response to a subject access request.

3.5 Health, education and social work records

The Council holds education and social work records to undertake its functions. The Council may also hold occupational health records for Council staff. There are only very limited reasons for withholding these records where a subject access request has been made, as explained below.

i. Personal data relating to an individuals' physical or mental health

In some instances, the applicant may not have seen this personal data (or may have only seen part of the records). This type of personal data may be exempt where the disclosure would be likely to cause serious harm to the physical or mental health of the individual themselves or any other person.

Before deciding whether this exemption under the DPA applies, the Council is obliged to consult the health professional responsible for the clinical care of the individual. It is the health professional's decision as to whether the health data can be disclosed and there is no discretion to disclose without a response from the health professional.

ii. Personal data contained within educational records

Certain educational data is exempt where:

a. disclosure would cause serious harm to the physical or mental health of the data subject or any other person, or

b. a parent (or someone with parental responsibility) or court appointee makes a request on behalf of a data subject, the data consist of information as to actual or potential child abuse and such compliance would not be in the interests of the data subject.

This exemption is found in the ***Data Protection Act 2018***

The author of the education record should be consulted prior to deciding whether to rely on this exemption.

iii. Personal data contained within social work records

Social work data is exempt where granting a subject access request would be likely to prejudice the carrying out of social work by virtue of resultant serious harm to the physical or mental condition of the data subject or any other person. The exemption does have limitation and can be found in the ***Data Protection Act 2018*****.** It also covers applications made on behalf of data subjects by those empowered by virtue of parental responsibility or by being a court appointee.

This type of personal data would be exempt from disclosure where the release is likely to prejudice the carrying out of social work because serious harm to the physical or mental health of the data subject or any other person could result from the disclosure.

The author of the social work record or lead social worker should be consulted prior to deciding whether or not to rely on this exemption.

If the request is for CYPS case records that have been closed for several years previous then the appropriate team to consult will be the team which was the individual's last point of contact with the department. For example if individual was previously on the child protection Register then the Family Support/Child Protection team should be consulted. Alternatively if the individual was previously in care then the Leaving Care Service should be consulted prior to any disclosure of information.

iv. Personal data held within occupational health reports

An employee (or former employee) may request access to their occupational health report. In such circumstances personal data can be exempt if the disclosure of the personal data is likely to cause serious harm to the physical or mental health of the data subject, or some other person.

The health professional who wrote the report should be consulted prior to relying on this exemption.

3.6 Health and Social Care Complaints – Regulatory Activity

Personal data processed in connection with complaints under the Health and Social Care (Community Health and Standards) Act 2003 is exempt from disclosure where the disclosure would be likely to prejudice the handling of the complaints under that Act.

3.7 Adoption Records (SI No. 1865 [2000])

Requests for access to adoption records are exempt from disclosure under the DPA. Any such requests should be handled in line with the provisions of the Adoption and Children's Act 2002.

The exemption is found in the ***Data Protection Act 2018***

If applicable this exemption means that individuals (including adopted people, birth relatives, adoptive parents and prospective adoptive parents) are not able to use the route of subject access to obtain information of this nature. It would be a breach of the DPA to allow such access under a SAR.

Essentially all the council's records held for adoption purposes are exempt from SAR provisions. There are special procedures for individuals to gain access to their adoption records – these will be well known to social work practitioners. The details vary by date of adoption.

Due to the nature of the information it will involve appropriate counselling of the individual and more considered approach to obtaining the data, ensuring the individual is helped through the process.

If an individual is seeking access to their adoption record they should contact ; The Adoption Contact Register

The following process should be followed:

1. The SAR should be logged as usual.
2. Does the SAR explicitly include a reference to Adoption Records?

Yes - adoption records only - (eg please send me a copy of all my adoption papers) - refuse this as a SAR as an exemption exists. Give the requester the appropriate information about how to make the request under the correct provisions.

Yes - as part of a request for other information that is not adoption records – (eg please let me have a copy of all environmental health records about my noise complaints and a copy of my adoption records) - deal with the non- adoption records as a standard SAR but refuse the adoption records as these are not covered by a SAR and this information is exempt. Give the requester the appropriate information about how to make the request under the correct provisions in the refusal part of the acknowledgement letter.

No - but their request is wide enough in scope to cover these – (eg provide me with a copy of all my social work records from when I was taken into care until I was 16). Deal with the non-adoption records as a standard SAR, do not disclose the adoption records as they are exempt **and do not refer to the existence of this information in the reply.** If the person has not explicitly referred to their adoption records they may not be aware of them and to use the exemption will inform them that there are adoption records.

No - and the request does not refer to them – (eg please send me a copy of all the emails I have had with the council about freedom of information requests) deal as a standard SAR and do not refer to the adoptions records or exemptions as this is out of scope.

3.8 References

Under the DPA 1998, the exemption only applied to references given. It did not apply to references received.

However, under the DPA 2018, this caveat was **not** included and that the reference giver and the reference receiver can rely on this exemption. A data subject has no access to such references.

3.9 Management forecasts and planning

Personal data processed for the purposes of management forecasting or management planning are exempt from subject access to the extent that disclosure would be likely to prejudice the planning or forecasting activity.

For example, information about plans to promote, transfer or make a worker redundant may be withheld if access would be likely to prejudice the conduct of the Council's business.

3.10 Negotiations

Personal data which contain a record of the intentions of the Council in relation to any negotiations with the individual are exempt from subject access to the extent that disclosure of that personal data would be likely to prejudice the Council's position in those negotiations.

For example, a statement outlining the maximum amount of money that the Council would be willing to give a data subject as an out of court settlement could be withheld under this exemption, whilst the negotiations are on-going.

Information about negotiations which have ended are unlikely to be exempt unless it can be shown that other on-going negotiations would be prejudiced by such a disclosure.

3.11 Legally professionally privileged information

If personal data consists of information in respect of which a claim to legal professional privilege could be maintained, then that data may be exempt.

Legal professional privilege applies to correspondence (e.g. letters, emails and memos) between Council employees and the Council's legal advisors (internal or external) for the purposes of obtaining legal advice.

For example this exemption could apply where an individual involved in litigation with the Council is requesting access to the personal data contained within the Council's legal advice file (from our internal or external lawyers).

Communications with Council's lawyers are likely to be subject to legal professional privilege and must not be disclosed. If such documents are found whilst dealing with a subject access request, seek advice from the legal adviser concerned.

3.12 What should you do if an exemption applies to the personal data?

If personal data is to be withheld under any of the exemptions then the reasons for the non-disclosure (including the exemption relied upon) should be documented on file so that the Council can justify its actions to the Information Commissioner or the courts. Such reasons should normally be provided to the applicant, as well as an explanation of the way the application of the exemption can be challenged.

The Crime and Taxation exemption does not have to be cited in your response to the applicant, if notifying the applicant of the reliance placed on this exemption would cause prejudice to the criminal investigation or taxation assessment/collection.

Where an exemption applies only in part, then the information which is not exempt should be released to the data subject within the statutory time frame.

3.13 Leaving Care records

Whilst there is no exemption under the Data Protection Act 2018, leaving Care files have been added to this section to address concerns and issues raised over their release where individuals seek information from their time in care.

Often accessing records of this nature can be a very positive experience, however sometimes the information contained within those records can be difficult to understand and in some cases upsetting.

Officers must be mindful that whilst the organisation has a legal obligation under the Data Protection Act to provide a Right of Access to information, this must be balanced with our legal duty of care, by managing the sensitivities of the information and the impact it may have on the individual and / or family members ensuring they are appropriately protected.

3.14 Historic Child Abuse

Lambeth Council has been supporting Operation Trinity, Scotland Yard's investigation into historic abuse cases in the Borough since November 2012. This has resulted in many subject access requests from the survivors of child abuse and there may be more in future.

In relation to incidents of historic abuse, Lambeth council has written to the Chair of The Independent Panel Enquiry into Child Sexual Abuse to make a formal offer to share with the inquiry the material that has been gathered with regard to historic child abuse in Lambeth. We also offered any other support needed to examine how individuals and organisations failed children in the past.

All requests on historic child abuse should be sent to the Historic SARS – Senior Project Lawyer/SARs.

Special arrangements exist in passing information held to the survivors of child abuse. All enquires regarding these arrangements should be referred to the Historic SARS team.

4. MONITORING SAR PERFORMANCE

The following steps will be taken to monitor subject access requests performance:

1. The number of 'subject requests' received, as well as the Council's compliance with the Data Protection Act, is monitored via by ***i-Casework***.
2. Weekly reports of subject requests received in the week to IAOs
3. Outstanding subject requests sent round on a weekly basis
4. Reports to CMT in the same format as used for the IGWG

5. USEFUL LINKS/RESOURCES

ICO Right of Access (Oct 2020)

https://lambeth.sharepoint.com/sites/InformationGovernanceNewVersion

Appendix 1 – Disclosing personal information to Elected Members

The role of the elected member

The elected members of a council are likely to have three different roles.

- They will represent residents of their ward, eg. in dealing with complaints.
- They will act as a Member of the Council, eg. as a member of a committee.
- They may represent a political party, particularly at election time.

Depending on the role the elected member has at any one time, the local authority may be able to disclose personal information on residents, staff, officials or contractors as long as the need to access and use of the information is to carry out official duties. In doing so, it will often be necessary to explicitly restrict the use of any personal information provided for official duties and to keep a record of the request.

Disclosures to the elected member as a Member of the Council

Local authorities can disclose personal information to an elected member if they need to access and use that information to carry out official duties. Elected members are, effectively, in the same position as an employee.

The local authority should consider the following:

- The elected member should only be given access to the personal information they need to carry out their duties.

For example, a member of the Housing Committee may attend a meeting to decide whether or not to seek the eviction of a council tenant. The local authority may provide them all the **relevant** personal information about the tenant and the circumstances giving rise to the possible eviction.
However, the local authority would not be justified in providing the elected member with general access to the Housing Department system.

- When disclosing personal information to the elected member, the local authority should specify the purposes for which that information may be used or disclosed.

- Where the elected member is able to take a copy of the personal information away from local authority premises (whether in paper or electronic form), or where they have remote access to the information, the local authority should specify the steps to be taken to keep the information secure.

Disclosures to elected members acting on behalf of local residents

A local authority does not generally have to get the consent of an individual to disclose their personal information to an elected member, as long as:

- the elected member represents the ward in which the individual lives;
- the elected member makes it clear that they are representing the individual in any request for their personal information to the local authority; **and**
- the information is necessary to respond to the individual’s complaint.

Where personal information is particularly sensitive, it may be advisable to get an individual's signed consent. However, there may be circumstances where the individual would reasonably expect their sensitive information to be disclosed to respond to their complaint. The basis for this processing is in the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 No. 2905.

NB In any event, when providing personal information to the elected member, the local authority should make clear that it is provided only to help the individual and must not be used for any other purpose. Any requests for personal data by an elected member should be logged by the relevant service area.

Disclosures to elected members for political purposes

Local authorities should not normally disclose personal information to elected members for political purposes without the consent of the individuals concerned.

There are two exceptions to this:

- There may be sets of personal information which the local authority is required to make public, for example, lists of some types of licence holder. In this case the Act does not prevent disclosure.

- Personal information may also be disclosed if it is presented in an aggregated form and does not identify any living individuals, for example, Council Tax band information or statistical information. However, there would be a breach of the Act if personal information was released in an apparently anonymised form which could then be linked to the individuals concerned, for example, by comparing property data with the electoral roll.

Appendix 2 – Guidance regarding request for data about the deceased

Information relating to deceased individuals is sometimes requested under the Subject Access provisions. Information relating to the deceased is not covered by the UK GDPR or the Data Protection Act and should not be treated as a Subject Access request. However the following guidance may prove useful when handling a request of this nature.

Deceased persons do not have subject access rights. This is because the UK GDPR and the DPA defines personal data as data which could lead to the identification of a (living) natural person. However, information about a deceased person could identify living persons in which case this would be personal data governed by the DPA.

A request for information about a deceased person can be treated as business as usual, a discrete disclosure or as a Freedom of Information Act (FOI) Request depending on the circumstances.

The FOI Act gives public access to information held by public authorities and a request made under the FOIA must be responded to. There are restrictions on the type of information that can be provided under FOI. A business-as-usual request is a request for day to day or service information which can usually be provided without any questions.

As a rule of thumb, where information cannot be provided without active consideration or under any other access regime, it should be processed under FOI.

Do not treat it as a business-as-usual request if the request for information:

i. is sensitive in any way,
ii. could lead to the identification of another person
iii. was received in confidence, or
iv. is available by other means (eg. a death certificate is a public document available from the Registrar's office; or there could be a right of access to the information under the Access to Health Records Act)

Appendix 3 – List of Deputy Information Asset Owners (DIAOs)

Children's Services

- **Director of Children's Commissioning and Community Safety**
- **Director of Children's Social Care**
- **Director of Education and Learning**

Finance and Investment

- **Director of Human Resources**
- **Director of Finance and Property**

Integrated Health and Adults

- **Assistant Director Finance (Adults and Health)**
- **Deputy Director – Adults Social Care**
- **Assistant Director – Adults Social Care**
- **Director of Integrated Commissioning (with CCG)**
- **Director of Public Health**

Legal and Governance

- **Assistant Director Inquiry Legal Team**
- **Deputy Democratic Services Manager**
- **Electoral Services Manager**
- **Head of Information Governance**
- **Principal Lawyer – Governance**
- **Principal Lawyer – Housing, Property and Planning**
- **Principal Lawyer – Social Care**

Resident's Services

- **Director of Infrastructure and Capital Delivery**
- **Director of Residents Experience and Digital**
- **Director of Environment and Streetscene**

Housing

- **Assistant Director of Home Ownership and Rents**
- **Assistant Director of Housing Needs**
- **Assistant Director of Housing Strategy and Performance**
- **Head of Compliance - Housing**

Strategy and Communication

- **Director of Strategy and Communication**

Strategy Growth and Opportunity

- **Director of Economy, Culture and Skills**
- **Director of Planning, Transport and Sustainability**
- **Director Regeneration and Housing Growth**

Appendix 4 – Data Protection Internal Review

Procedure Data Protection Complaints Procedure

Summary –

Requests to review decisions made under the Data Protection Act are not dealt with at stage 2 of the Corporate Complaints Policy.

In order to ensure that the request to review a decision is processed properly, the procedure is as follows:

The person(s) involved in making the initial decision should not be involved in the review. The aim is to ensure that there is a fair and thorough review of handling issues and decisions taken in relation to the Act. Due to this the officer responsible for undertaking the review, will be either:

- The IG Team **OR** the Head of Information Governance

1. All requests for internal reviews of subject access responses (i.e. any expression of dissatisfaction or complaint) should be directed to the data protection (dataprotection@lambeth.gov.uk). The request will be logged on the ***iCasework*** database

2. The officer handling the review (or their delegate) will acknowledge the request for review, within 2 working days and provide the complainant with the target response date.

3. The officer will action the request within 20 working days, notify the officers who handled the original request of the outcome, record the response and close the case on ***i-Casework***.

The response to the complainant should include:

- A thorough re-evaluation of all the issues relevant to their complaint
- Where the outcome of the complaint is a decision that information should be disclosed where it was previously withheld, the information in question should be disclosed at the same time the response to the complainant is sent. If this is not practicable, the applicant should be informed of the timescale for the information being sent to them.

- Where the outcome of the complaints is that the initial decision to withhold the information is upheld, then the complainant should be informed of their right to apply to the Information Commissioner for an independent review.

Appendix 5 – DPA Exemptions summary

<table>
<tr><th>Type of exemption</th><th>How to apply it</th></tr>
<tr><td>Documents containing information about another person (Third Party)</td><td>Where information relates not only to the individual making the request, but also to another individual, you do not need to comply with a request if doing so will mean that information relating to another individual would be disclosed, except where:
the other individual has consented to the disclosure, or
it is reasonable in all the circumstances to disclose the information without that individual’s consent.
In deciding whether it may be reasonable to disclose the following should be considered: -

a) any duty of confidentiality owed to the other individual,
b) whether you feel it necessary to seek consent of the other individual,
c) whether the other individual is capable of giving consent, and
d) any express refusal of consent by the other individual.

You should also consider whether the information in question is already known to the individual, or whether it is possible to undertake a partial redaction allowing you to disclose the information without identifying the individual</td></tr>
<tr><td>Documents written by another person (Third Party)</td><td>Where a document is written by another person or organisation these are not automatically exempt.
Whilst the council is allowed to seek a view from the author of the document, it is the council’s decision whether to disclose or not. Before applying this exemption you should take into account the following:
Does the document contain information already known to the requester?
Is it likely the requester would have already received a copy?
Is there anything contentious in the document that is likely to cause concern if disclosed?
Has that document been marked in any way to indicate that disclosure is not allowed?</td></tr>
<tr><td>Legally privileged information</td><td>Personal data is exempt if it consists of information for which legal professional privilege (LPP) could be maintained in legal proceedings. The LPP exemption is fairly narrow and cannot be applied to all legal documentation.
The actual content of the information is important when considering this as an exemption, just the mere fact that it is a communication with a lawyer / solicitor does not make the document legally privileged.</td></tr>
</table>

	LPP can be applied to documents created on instructing a lawyer or as a result of advice being given or sought for the use in a legal case or in anticipation of a legal case. • Litigation privilege applies to confidential communications made for the purpose of providing or obtaining legal advice about proposed or contemplated litigation. There must be a real prospect or likelihood of litigation, rather than just a fear or possibility. • Advice privilege applies where no litigation is in progress or contemplated. It covers confidential communications between the client and lawyer, made for the main purpose of seeking or giving legal advice.
Social work	Social work data is exempt where granting a subject access request would be likely to prejudice the carrying out of social work by virtue of resultant serious harm to the physical or mental condition of the data subject or any other person. The exemption does have limitations, however if you are concerned that disclosure of information will put the case at risk and hinder the "social work process", this can be considered.
Serious harm to physical or mental health or condition	Health data is exempt where granting a subject access request would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person. This exemption only applies in the most serious cases and can only be used in consultation with an appropriate medical professional.
Management information	Personal data processed for the purposes of management forecasting or planning is exempt where disclosure would be likely to prejudice the conduct of that business or other activity of the council.
Educational records	Certain educational data is exempt where: • disclosure would cause serious harm to the physical or mental health of the data subject or another person, or • a parent (or someone with parental responsibility) or court appointee makes a request on behalf of a data subject, the data consist of information as to actual or potential child abuse and such compliance would not be in the interests of the data subject.

Adoption Records	Adoption records held by the council are exempt from the subject access provisions. If applicable this exemption means that individuals (including adopted people, birth relatives, adoptive parents and prospective adoptive parents) are not able to use the route of subject access to obtain information of this nature. It would be a breach of the DPA to allow such access under a SAR. There are special procedures for individuals to gain access to their adoption records. Due to the nature of the information it will involve appropriate counselling of the individual and more considered approach to obtaining the data, ensuring the individual is helped through the process.

Appendix 6 – CCTV Subject Access Request

https://beta.lambeth.gov.uk/about-council/privacy-data-protection/subject-access-requests

Appendix 6 - DATA SUBJECT RIGHTS

1. The right to withdraw consent

The data subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (i.e. the processing is not based on a different justification allowed by the UK GDPR/DPA such as contractual, legal obligation or public task).

Before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the legal basis of the processing. If not, then the request may be rejected on the grounds that the processing does not require the data subject's consent. Otherwise, the request should be allowed.

In many cases, the giving and withdrawal of consent will be available electronically (i.e. online via email to unsubscribe or withdraw consent to appropriate service area), and this procedure will not be required.

Where consent involves a child the giving or withdrawal must be authorised by the holder of parental responsibility over the child.

For more information on Consent, see Lambeth Council's Data Protection Policy.

2. The right of access - commonly referred to as 'Subject Access Request' (SAR)

A data subject has the right to ask Lambeth Council whether we process data about them and to have access to such data. The right of access gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their date, and check that we are doing it lawfully.

In most cases, the decision-making process for such requests will be straightforward unless it is judged that the request is manifestly unfounded or excessive. The compilation of the information is likely to require the input of the relevant directorate DIAO.

For more information on how to proceed with a right of access subject request, see the 'Handling a Subject Request' section 3.2 below.

4. The right to rectification

Where personal data is inaccurate, the data subject has the right to request that it be corrected and incomplete personal data completed based on information they may provide.

Where necessary, Lambeth Council will take steps to validate the information provided by the data subject to ensure that it is accurate before amending it.

If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

The DPA states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

As a matter of good practice, you should restrict the processing of the personal data in question whilst you are verifying its accuracy, whether or not the individual has exercised their right to restriction.

If you are satisfied that the data is accurate however, you should let the individual know. You can also refuse to comply with a request to rectify if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either request a 'reasonable fee' to deal with the request or refuse the request. You should explain your decision, and inform them of the right to make a complaint to the ICO.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

3. The right to erasure

Also known as "the right to be forgotten", the data subject has the right to require Lambeth Council to erase personal data about them without undue delay where one of the following applies:

- The personal data are no longer necessary for the purpose for which they were collected
- The data subject withdraws consent and there is no other legal ground for processing
- You are relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- You have to delete it to comply with a legal obligation
- The data subject objects to the processing of the personal data (i.e. for direct marketing purposes)
- The personal data have been unlawfully processed

Reasonable efforts must be made to ensure erasure where the personal data has been made public or shared with 3rd parties.

If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of the data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

Lambeth Council will need to make a decision on each case of such requests as to whether the request can or should be declined for one of the following reasons:

- Right of freedom of expression and information
- Compliance with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority (public task)
- To protect archiving purposes, scientific or historical research or statistical purposes in the public interest
- The personal data is relevant to a legal claim

It is likely that such decisions will require the involvement of the Data Protection Officer.

You can also refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either request a ‘reasonable fee’ to deal with the request or refuse the request. You should explain your decision, and inform them of the right to make a complaint to the ICO.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

4. The right to restrict processing

The data subject can exercise the right to a restriction of processing of their personal data in one of the following circumstances:

- Where the data subject contests the accuracy of the data, until we have been able to verify its accuracy
- As an alternative to erasure in the circumstances that the processing is unlawful
- Where the data subject needs the data for legal claims but it is no longer required by us
- Whilst a decision on an objection to processing is pending

Lambeth Council will need to make a decision on each case of such requests as to whether the request should be allowed.

Where a restriction of processing is in place, the data may be stored but not processed without the data subject’s consent, unless for legal reasons (in which case the data subject must be informed). Other organisations who may process the data on our behalf must also be informed of the restriction.

Although distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- If an individual has challenged the accuracy of their data and asked you to rectify it, they also have the right to request you restrict processing while you consider their rectification request; or
- If an individual exercises their right to object, they also have a right to request you to restrict processing while you consider their objection request.

The definition of processing includes a broad range of operations including collection, structuring, dissemination, sharing and erasure of data. You must not process the restricted data in any way except to store it. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

The UK GDPR suggests a number of methods that could be used to restrict data, such as:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from a website.

If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction of the personal data – unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction. If you do this, you must inform the individual before you lift the restriction and keep a record of your decision.

You can also refuse to comply with a request for restriction if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either request a 'reasonable fee' to deal with the request or refuse the request. You should explain your decision, and inform them of the right to make a complaint to the ICO.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

5. The right to data portability

The data subject has the right to request that their personal data be provided to them in a "structured, commonly-used and machine-readable format" (GDPR Article 20) and/or to transfer that data to another party e.g. service provider.

Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you (i.e. not received from other sources or that you have created based on the data an individual has provided to you).

This right will rarely apply to Lambeth Council as it **only applies to the lawful bases of consent or the performance of a contract**.

Where applicable, the data subject can also request that the personal data be transferred directly from our systems to those of another provider.

For services that come under this category, little decision-making is required for each case and it is highly desirable that this process is automated in its execution.

You can also refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either request a 'reasonable fee' to deal with the request or refuse the request. You should explain your decision, and inform them of the right to make a complaint to the ICO.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

6. The right to object

The data subject has the right to object to processing that is based on the following legal justifications:

- For the performance of a task carried out in the public interest or in the exercise of official authority vested in Lambeth Council
- For the purposes of the legitimate interests of Lambeth Council (or those of a third party)

The right is not absolute. If you are processing the data based on the individual's consent or for scientific or historic research, or statistical purposes, the right to object is more limited.

You can also continue processing if:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Once an objection has been made, Lambeth Council must justify the grounds on which the processing is based and suspend processing until this is done. Where the personal data is used for direct marketing we have no choice but to no longer process the data.

However, this does not mean that you need to erase the individual's personal data, and in most cases it will be preferable to suppress the details. Suppression involves retaining enough information about them to ensure that their preference not to receive direct marketing is respected in the future.

You can also refuse to comply with an objection to processing if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either request a 'reasonable fee' to deal with the request or refuse the request. You should explain your decision, and inform them of the right to make a complaint to the ICO.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

7. Rights in relation to automated decision-making and profiling

The data subject has the right to not be the subject of automated decision-making where the decision has a significant effect on them, and can insist on human intervention where appropriate. The data subject also has the right to express their point of view and contest decisions.

There are exceptions to this right, which are if the decision:

- Is necessary for the entry into or performance of a contract
- Is authorised by law
- Is based on the data subject’s explicit consent

If your processing falls under the above definition of automated decision-making and profiling, you must:

- Consider carrying out a Data Protection Impact Assessment (DPIA);
- Give individuals information about the processing (including the lawful basis);
- Introduce simple ways for them to request human intervention or challenge a decision;
- Carry out regular checks to make sure that your systems are working as intended.

In assessing these types of request, a judgment needs to be made about whether the above exceptions apply in the particular case in question.

END