



HASLEMERE TOWN COUNCIL

Subject Access Request Procedure

1. Purpose	3
2. Scope	3
3. Definition	3
4. Responsibilities	3
4.2 Data Protection Officer / Data Protection Adviser	4
4.3 Councillors and Staff	4
5. How a Subject Access Request May Be Made	4
6. Receiving and Logging the Request	4
7. Identity Checks	5
7.1 When ID may be requested	5
7.2 Acceptable ID	5
7.3 Representatives	5
8. Clarifying the Request	5
9. Timeframe	6
9.1 Extension	6
10. Fees	6
11. Searching for Information	6
12. Reviewing the Information	7
13. Third-Party Data and Redaction	7
14. Exemptions and Restrictions	7
15. Format of Response	8
16. Contents of the Response	8
17. Refusal or Partial Refusal	8
18. Internal Record Keeping	9
19. Preservation of Records	9
20. Complaints	9
21. Template Acknowledgement	9
22. Template ID Request	10
23. Template Response Letter	10

1. Purpose

This procedure sets out how **[Name of Council]** will handle requests made by individuals seeking access to their personal data under **Article 15 UK GDPR** and the **Data Protection Act 2018**.

The Council will respond to subject access requests **without undue delay and in any event within one month**, subject to any lawful pause while awaiting ID or clarification, and any lawful extension where the request is complex or numerous. The DPA 2018 also requires councils to facilitate data subject rights and sets out the applicable one-month period in related access provisions **【】** .

2. Scope

This procedure applies to:

- all subject access requests made to the Council by current or former employees, councillors, residents, tenants, allotment holders, contractors, complainants, correspondents or any other individual;
- requests made in writing, by email, by letter, via social media, by hand, or verbally where sufficiently clear;
- all personal data held by the Council in electronic, paper, audio, visual or other formats.

This procedure does **not** apply to:

- requests for non-personal information under the Freedom of Information Act 2000;
- routine requests for publicly available documents;
- requests made by third parties unless authority to act has been verified.

3. Definition

A **Subject Access Request (SAR)** is a request by an individual for:

- confirmation that their personal data is being processed;
- access to their personal data; and
- the supplementary information required by Article 15 UK GDPR.

Under the DPA 2018, a data subject access right includes the right of access under Article 15 GDPR **【】** .

4. Responsibilities

4.1 Clerk / Proper Officer

The Clerk is responsible for:

- logging the request;
- coordinating searches;
- verifying identity where needed;
- reviewing the information gathered;

- seeking legal or data protection advice where necessary;
- issuing the response; and
- maintaining a record of the request and outcome.

4.2 Data Protection Officer / Data Protection Adviser

Where the Council has a DPO or retained adviser, they should be consulted on:

- complex requests;
- redactions and exemptions;
- third-party data issues;
- requests involving special category or employment data;
- refusal decisions; and
- extensions of time.

4.3 Councillors and Staff

All councillors and staff must:

- forward any SAR to the Clerk immediately;
- preserve relevant records;
- carry out searches when asked;
- not delete, alter, conceal or destroy information after a request is received.

The DPA 2018 makes it an offence to alter, erase, destroy or conceal information to prevent disclosure to a person exercising a data subject access right **【1】**.

5. How a Subject Access Request May Be Made

A SAR does not need to mention “subject access request”, “Article 15” or “UK GDPR”. Any communication should be treated as a SAR if an individual is clearly asking for their own personal data.

Examples:

- “Please send me all the information you hold about me.”
- “I want copies of emails about me.”
- “What personal data do you hold on my allotment complaint?”

If unclear, the Council should promptly seek clarification.

6. Receiving and Logging the Request

On receipt of a SAR, the Clerk must:

1. record the date received;

2. log the requester's name and contact details;
3. note how the request was received;
4. summarise what information is being sought;
5. allocate a reference number;
6. acknowledge receipt promptly;
7. consider whether ID is needed;
8. consider whether clarification is needed to locate the data efficiently.

A request should be acknowledged as soon as possible, ideally within **2 to 5 working days**.

7. Identity Checks

The Council may ask for additional information where it has reasonable doubts about the requester's identity. The DPA 2018 expressly allows a controller to request additional information to confirm identity and delay dealing with the request until identity is confirmed **【】**.

7.1 When ID may be requested

ID may be requested where:

- the requester is unknown to the Council;
- the request is made from an unfamiliar email address;
- sensitive or extensive data is involved;
- a third party is acting on behalf of the individual.

7.2 Acceptable ID

Examples include:

- passport or driving licence; and/or
- recent utility bill or bank statement showing address.

The Council should request only the minimum evidence needed.

7.3 Representatives

If a solicitor, family member or other representative makes the request, the Council must obtain:

- written authority signed by the data subject; and
- proof of identity as appropriate.

8. Clarifying the Request

If the request is broad, the Council may ask the requester to clarify the scope, for example:

- date ranges;
- subject matter;
- names of services, facilities or committees;

- whether specific correspondence is sought.

The Council should still begin reasonable searches and should not delay unnecessarily. Clarification is to help locate the data, not to obstruct the request.

9. Timeframe

The Council must respond **without undue delay and within one month** of the relevant start date.

The relevant date will usually be the latest of:

- the date the request was received; and
- the date any reasonably required ID or clarification needed to process the request was received.

For related access rights under the DPA 2018, the applicable time period is one month beginning with the latest of receipt of the request, receipt of additional identifying information, or payment of any lawful fee **【】**.

9.1 Extension

The Council may extend the response period by up to **two further months** where the request is complex or numerous. If so, the requester must be informed within the first month and given reasons.

10. Fees

SARs will normally be handled **free of charge**.

A reasonable fee may only be charged where a request is **manifestly unfounded or excessive**, or for further copies in limited circumstances. The DPA 2018 confirms that manifestly unfounded or excessive requests may justify a reasonable fee or refusal, and the burden is on the controller to show this **【】**.

Any decision to charge a fee must be approved by the Clerk in consultation with the DPO or legal adviser.

11. Searching for Information

The Clerk will coordinate reasonable and proportionate searches of all relevant systems, which may include:

- Council email accounts;
- committee and meeting records;
- complaint files;
- allotment, cemetery or hall booking records;
- personnel records;
- finance or debtor records;
- correspondence files;

- handwritten notes where they form part of a relevant filing system;
- cloud storage, shared drives and archived files;
- CCTV footage, where applicable.

Searches should be limited to personal data belonging to the requester and relevant to the request.

12. Reviewing the Information

Once gathered, the material must be reviewed to determine:

- whether it contains the requester's personal data;
- whether any exemptions apply;
- whether third-party personal data appears;
- whether redactions are required;
- whether any information is legally privileged, confidential or otherwise restricted.

The Council is not required to disclose information that falls outside the scope of the access right or is exempt under the Data Protection Act 2018.

13. Third-Party Data and Redaction

Where documents contain personal data of other individuals, the Council must consider whether it is reasonable to disclose that information.

The Council should normally:

- redact third-party names and identifying details unless consent has been obtained or disclosure is otherwise reasonable and lawful;
- consider whether the third party is acting in an official or professional capacity;
- consider confidentiality expectations and potential impact.

All redactions should be clearly marked and recorded.

14. Exemptions and Restrictions

The Council may withhold some information where a lawful exemption applies under the Data Protection Act 2018, including where disclosure would:

- prejudice the rights and freedoms of others;
- reveal legally privileged material;
- disclose confidential references, where exempt;
- prejudice negotiations or regulatory functions, where relevant exemptions apply.

Any reliance on an exemption must be:

- considered carefully;
- limited only to the specific information covered; and

- recorded with reasons.

Complex exemption decisions should be referred for legal or DPO advice.

15. Format of Response

The Council must provide the response in a **concise, intelligible and easily accessible form**, using clear and plain language. The DPA 2018 requires this standard and says the information should, where practicable, be provided in the same form as the request **【】**.

Responses may be sent:

- by secure email;
- by encrypted electronic transfer;
- by printed copy;
- by supervised inspection, if appropriate.

The format should take account of the requester's needs and accessibility requirements.

16. Contents of the Response

The response should include:

1. confirmation whether personal data is being processed;
2. a copy of the requester's personal data;
3. supplementary information, including:
 - purposes of processing;
 - categories of personal data;
 - recipients or categories of recipient;
 - retention period or criteria;
 - right to rectification, erasure, restriction and objection where applicable;
 - right to complain to the ICO;
 - source of the data if not collected from the individual;
 - any safeguards for international transfers, where applicable.

17. Refusal or Partial Refusal

If the Council refuses to comply, wholly or partly, it must inform the requester:

- of the refusal and the reasons, unless an exemption allows that also to be withheld;
- of their right to complain to the ICO; and
- of their right to seek a judicial remedy.

Any refusal must be approved by the Clerk and, where appropriate, the DPO or legal adviser.

18. Internal Record Keeping

For each SAR, the Council will keep an internal record including:

- SAR reference number;
- requester name;
- date received;
- date acknowledged;
- ID requested/received;
- clarification requested/received;
- searches undertaken;
- systems searched;
- exemptions considered;
- redactions made;
- date response issued;
- outcome;
- any lessons learned.

This record should be retained in line with the Council's retention arrangements.

19. Preservation of Records

Once a SAR is received, relevant records must not be destroyed, deleted, overwritten or amended except through normal documented processes unrelated to the request and only where lawful.

If there is any risk of deletion, the Clerk should issue a temporary "hold" instruction to relevant councillors, staff or contractors.

20. Complaints

If a requester is dissatisfied, they should first be invited to contact the Clerk so the matter can be reviewed.

They must also be informed of their right to complain to the **Information Commissioner's Office (ICO)**.

21. Template Acknowledgement

Subject: Subject Access Request Acknowledgement

Dear [Name],

Thank you for your request received on [date], in which you asked for access to personal data held by [Name of Council].

We are treating your correspondence as a Subject Access Request under data protection legislation.

We will respond without undue delay and normally within one calendar month of receipt of your request. If we require proof of identity or further clarification in order to process your request, we will let you know as soon as possible.

If you would like to narrow or clarify your request, for example by giving relevant dates, subjects or types of records, this may help us locate the information more efficiently.

Yours sincerely,
[Name]
Clerk / Proper Officer
[Council]

22. Template ID Request

Subject: Subject Access Request – Proof of Identity Required

Dear [Name],

Thank you for your request for access to personal data held by [Name of Council].

Before we can process your request, we need additional information to confirm your identity. This is to ensure that personal data is disclosed only to the correct person.

Please provide [one photo ID and one proof of address / suitable alternative].

Once we receive this information, we will continue processing your request.

Yours sincerely,
[Name]
Clerk / Proper Officer

23. Template Response Letter

Subject: Response to Subject Access Request

Dear [Name],

I write further to your Subject Access Request received on [date].

[Name of Council] confirms that it [does/does not] process personal data relating to you.

Please find enclosed/attached:

- a copy of the personal data we hold which falls within the scope of your request; and
- the information required about how and why your personal data is processed.

Summary information

- **Purposes of processing:** [insert]
- **Categories of personal data:** [insert]
- **Recipients/categories of recipients:** [insert]
- **Retention period/criteria:** [insert]
- **Source of data:** [insert if applicable]

Some information has been withheld or redacted because [brief explanation: e.g. it includes third-party personal data / an exemption applies].

If you are dissatisfied with this response, please contact [Clerk contact details]. You also have the right to complain to the Information Commissioner's Office at www.ico.org.uk.

Yours sincerely,

[Name]

Clerk / Proper Officer