Ashdon Parish Council

Subject Access Request (SAR) Procedure

1. SUBJECT ACCESS REQUESTS ("SAR") BASIC REQUIREMENTS

A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted.

B. Make sure a SAR policy is in place within the council and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:

(1) Responsibilities (who, what)
(2) Timing
(3) Changes to data
(4) Handling requests for rectification, erasure or restriction of processing.

C. Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

D. Where possible, implement standards to respond to SARs, including a standard response.

2. SUBJECT ACCESS REQUESTS PROCEDURE FOR ASHDON PARISH COUNCIL (APC)

A. What must APC do?

1. MUST: On receipt of a subject access request, the Clerk will inform the Chair &/or Vice-Chair.
2. MUST: The Clerk (in conjunction with the Chair must correctly identify whether a request has been made under the Data Protection legislation
3. MUST: The Clerk, and as appropriate, Chair &/or Vice-Chair, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive search of the records to which they have access.
4. MUST: All the personal data that has been requested must be provided unless an exemption can be applied.
5. MUST: APC must respond within one calendar month after accepting the request as valid.
6. MUST: Subject Access Requests must be undertaken free of charge to the requestor unless the legislation permits reasonable fees to be charged.
7. MUST: Councillors and managers must ensure that the staff they manage are aware of and follow this guidance.
8. MUST: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint.

3. HOW MUST THIS BE UNDERTAKEN?

3.1 Notify the Chair &/or Vice Chair upon receipt of a request.

3.2. APC must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. APC should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. This evidence must be dated in the past 12 months.

3.3 Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

3.4 APC must not withhold personal data because it believes it will be misunderstood; instead, APC should provide an explanation with the personal data. APC must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. APC may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. APC must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

3.5 Make this clear on forms and on the council website.

3.6 APC will maintain a database allowing the council to report on the volume of requests and compliance against the statutory timescale.

3.7 When responding to a complaint, APC must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

4. RESPONSE TO SAR–SAMPLE LETTERS

1. All letters must include the following information:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom personal data has been
or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules;
(d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with the Information Commissioners Office ("ICO");
(g) if the data has not been collected from the data subject: the source of such data;
(h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Adopted 16th September 2024 - reviewed annually, next review due September 2025.