



Chattisham and Hintlesham Parish Council SUBJECT ACCESS REQUEST (SAR) PROCEDURE

1. FIRST STEPS

- 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 SARs are accurate and complied with. Include, provisions on: i. Responsibilities (who, what) ii. Timing iii. Changes to data iv. 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. THE PROCEDURE

- a) MUST: on receipt of a subject access request, the Clerk will inform the Chair &/or Vice-Chair of its receipt
- b) MUST: correctly identify whether a request has been made under the Data Protection legislation
- c) 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.
- d) MUST: All the personal data that has been requested must be provided unless an exemption can be applied.
- e) MUST: respond within one calendar month after accepting the request as valid.
- f) MUST: Subject Access Requests must be undertaken free of charge to the requestor unless the legislation permits reasonable fees to be charged.
- g) 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?

a) Notify the Chair &/or Vice-Chair upon receipt of a request

b) Chattisham and Hintlesham Parish Council 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. We should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity.

The Council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence / Shotgun Certificate
- EEA National Identity Card
- Full UK Paper Driving Licence
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*
- State/Local Authority Educational Grant Document*
- HMRC Tax Notification Document
- Disabled Driver's Pass or Financial Statement issued by bank, building society or credit card company+
- Judiciary Document such as a Notice of Hearing, Summons or Court Order
- Utility bill for supply of gas, electric, water or telephone landline +
- Most recent Mortgage Statement Most recent council Tax Bill/Demand or Statement
- Tenancy Agreement
- Building Society Passbook which shows a transaction in the last 3 months and your address

c) Depending on the degree to which personal data is organised and structured, we 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, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

d) We must not withhold personal data because we believe it will be misunderstood; instead, we should provide an explanation with the personal data. We 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. We may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. We must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

e) Make this clear on forms and on the Council website

f) Chattisham and Hintlesham Parish Council will maintain a database allowing the Council to report on the volume of requests and compliance against the statutory timescale

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

4. RESPONSE TO SUBJECT ACCESS REQUEST - SAMPLE LETTERS

All letters must include the following:

a) the purposes of the processing;

b) the categories of personal data concerned; Status

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 Rules¹ or EU model clauses ².

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.

¹ "Binding Corporate Rules" is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation's headquarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

² "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between