Godalming
Town Council
Supporting Our Community

Subject Access Policy, Procedures and Template Response Letters

Subject Access Requests Policy

1. Upon receipt of a Subject Access Request (SAR) Godalming Town Council will:

(a) Verify whether it is the controller of the data subject's personal data. If it is not a controller, but merely a processor, the Council will inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject. If needed, the Council will request further evidence on the identity of the data subject.

(c) Verity the access request. The Council will establish if the request is sufficiently substantiated and determine whether the SAR is clear regarding what personal data is requested. If the Council is uncertain of what data is required, it will request additional information from the data subject.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character). If so, the Council may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether the Council processes the data requested. If the Council does not process any data it will inform the data subject accordingly. The Council will, at all times ensure the internal SAR policy is followed and progress is monitored.

(g) Ensure data is not changed as a result of the SAR. However, routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and will make sure this data is filtered before the requested data is supplied to the data subject. If data cannot be filtered, the Council will ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. Responding to an SAR

(a) Godalming Town Council will respond to an SAR within one month after receipt of the request, however:

(i) if more time is needed to respond to complex requests an extension of another two months is permissible. The Council will communicate this to the data subject as soon as possible after the need for an extension of time becomes apparent, but within the first month;

(ii) if the Council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If an SAR is submitted in electronic form, the Council will aim to respond using the same means.

(c) Where data on the data subject is processed, the Council will provide the following information in the SAR response:

(i) the purposes of the processing;
(ii) the categories of personal data concerned;
(iii) 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[1] or EU model clauses[2];
(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
(v) 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;
(vi) the right to lodge a complaint with the Information Commissioner's Office ("ICO");
(vii) if the data has not been collected from the data subject, the source of such data;
(viii) 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.

(d) Provide a copy of the personal data undergoing processing.

[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 two data controllers or a data controller and a data processor.

Procedure to be followed on Receipt of a Subject Access Request

A Subject Access Request may be received by any member of staff or Councillor, therefore, all staff and Councillors are to be aware of the following procedure:

On receipt of a Subject Access Request the following actions must be done:

1. ***MUST***: On receipt of a subject access request, the person receiving it must **forward** it immediately to the Town Clerk, copied to the Support Services Officer.
2. ***MUST***: Correctly **identify** whether a request has been made under the Data Protection legislation.
3. ***MUST***: Any member of staff, and as appropriate, Councillor, who receives a request to locate and supply personal data relating to an 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***: **Respond** within one calendar month after accepting the request as valid.
6. ***MUST***: the Subject Access Requests must be undertaken **free of charge** to the requester 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 requester is not satisfied with a response to an SAR, the Council must manage this as a **complaint**.

In Managing a Subject Access Request the Town Clerk (or in his/her absence the Support Services Officer) must:

1. Notify the Chairman of the Audit Committee upon receipt of a request.
2. 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.
3. Clarify with the requester 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
    - 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.

4. Depending on the degree to which personal data is organised and structured, 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 the Council, or where appropriate individual Councillors, have responsibility for or owns.
5. Not withhold personal data because it is believed it will be misunderstood; instead, an explanation should be provided with the personal data. Personal data must be provided 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. The Council may seek to agree with the requester that the personal data will be viewed on screen or that files will be inspected in the Council's offices. Exempt personal data from the released documents will be redacted and an explanation of why that personal data is being withheld is to be provided.
6. Make this clear on forms and on the Council website.
7. Achieve this through the use of induction, by performance and training, as well as through establishing and maintaining appropriate day to day working practices.
8. Maintain a database allowing the Council to report on the volume of requests and compliance against the statutory timescale.
9. When responding to a complaint, the Council must advise the requester that they may complain to the Information Commissioner's Office ("ICO") if they remain unhappy with the outcome.

Sample Letters to be used in Responding to a Subject Access Request

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[3] or EU model clauses[4];
(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.

[3] "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.
[4] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

2. Replying to a Subject Access Request Providing the Requested Personal Data

[Date]

[Name]
[Address]

Dear [Name of data subject]

Data Protection Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the Council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

3. Release of part of the personal data, when the remainder is covered by an exemption

[Date]

[Name]
[Address]

Dear [Name of data subject]

Data Protection Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the Council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

4. Replying to a Subject Access Request explaining why you cannot provide any of the requested personal data

[Date]

[Name]
[Address]

Dear [Name of data subject]

Data Protection Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the Council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the Council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the Council should set out the reason why some of the data has been excluded.]

Yours sincerely