STILLINGFLEET PARISH COUNCIL

SUBJECT ACCESS REQUEST PROCEDURE

Subject Access Requests ("SAR")

Under the General Data protection regulations (GDPR) all data controllers must inform data subjects of their right to access their data and provide an easily accessible mechanism through which such a request can be submitted. Stillingfleet Parish Council (the Council) as a data controller intends to satisfy these requirements by having a SAR policy in place within the council so that internal procedures on handling of SARs are accurate and complied with.

The following procedure sets out what the Council should do on receipt of a SAR

What must the Council do?

1. ***MUST***: On receipt of a SAR it should be forwarded immediately to the Clerk to the Council and the Council's Chairman

2. ***MUST***: The Clerk to the Council must correctly **identify** whether a request has been made under the Data Protection legislation

3. ***MUST***: The Clerk to the Council, and as appropriate, all councillors, who receive 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***: The Council must ensure all 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.

5. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.

6. ***MUST***: The Council must **respond** within one calendar month after accepting the request as valid.

7. ***MUST***: SARs must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.

8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

How must the Council do it?

1. Notify clerk@stillingfleetparishcouncil.org upon receipt of a request.
2. The Clerk 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. The Clerk 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*
- HMRC Tax Notification Document
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company+
- Utility bill for supply of gas, electric, water or telephone landline+
- 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

3. Depending on the degree to which personal data is organised and structured, the Clerk and/or the Councillors 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 the Council is responsible for or owns.

4. The Council must not withhold personal data because it believes it will be misunderstood; instead, it should provide an explanation with the personal data. The Council 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. The Council must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. The Council must make it clear on the council's website how a SAR can be submitted.

6. The Council should maintain a database enabling the council to report on the volume of requests and compliance with the statutory timescale.

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

Upon receipt of a SAR

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

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you 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 you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. 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 make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

Responding to a SAR

(i) Respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

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

(j) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(k) If data on the data subject is processed, make sure to include as a minimum 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 Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data must be stated.

Policy Review:

This policy will be reviewed annually or at any other time the council requires.

111 "Binding Corporate Rules" is a global data protection policy covering the international transfer pf 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 organisations head quarters 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.

Signed on behalf of Stillingfleet Parish Council	Name	Date of Parish Council meeting at which this policy was adopted
	PAUL ELMHIRST CHAIRMAN	7 February 2019