Kirkby Malzeard, Laverton & Dallowgill Parish Council
Subject Access Requests (SAR) Policy

What must the Council do?

1. ***MUST***: On receipt of a subject access request **forward** it immediately to the Data Controller (Clerk).
2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation
3. ***MUST***: When the Data Controller receives a request to locate and supply personal data relating to a SAR they must make a full exhaustive **search** of all Council records.
4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. ***MUST***: We 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***: The Data Controller must ensure that all Councillors 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**.

How must the Data Controller (DC) do it?

1. Notify all Councillors 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. 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
    - 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
3. Depending on the degree to which personal data is organised and structured, the D.C. 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 D.C. must not withhold personal data because they believe it will be misunderstood; instead, they should provide an explanation with the personal data. The D.C. must provide the personal data in an "intelligible form", which includes providing 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 D.C. may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. The D.C. must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear within the response letters used and on the council website (achieved by the publication of this document). The D.C. will use the template response letters provided within Appendix 7 of the NALC GDPR Toolkit and will incorporate 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[1] 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.

6. The D.C. will be made familiar with this procedure during their initial induction, regular performance and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database will be created to enable the council to report on the volume of requests and compliance against the statutory timescale.

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

Adopted May 2019

[1] "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.