TIDENHAM PARISH COUNCIL

GENERAL DATA PROTECTION REGULATION (GDPR) May 2018

SUBJECT ACCESS REQUESTS POLICY

What must the Council do?

1. ***MUST***: On receipt of a subject access request this must be **forwarded** immediately to the Clerk
2. ***MUST***: The Clerk must correctly **identify** whether a request has been made under the Data Protection legislation
3. ***MUST***: A member of staff, and as appropriate, councillor, who receives a request from the Clerk 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***: The Council 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**.

How must this be done?

1. Notify the Clerk upon receipt of a request.
2. A request must be received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. It should be clarified 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, it will be necessary 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 Clerk, other members of staff or councillors are responsible for or own.

4. Personal data must not be withheld because it is believed it will be misunderstood; instead, an explanation should be provided with the personal data. The 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. It may be possible to agree with the requester that they will view the personal data on screen or inspect files on council premises. Exempt personal data must be redacted from the released documents and an explanation given as to why that personal data is being withheld.

5. This process must be made clear on forms and on the council website.

6. This process should be managed through induction and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database should be maintained allowing the Council to report on the volume of requests and compliance against the statutory timescale.

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

Subject Access Requests response 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[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.

2. **Changes to this policy**

   We keep this Subject Access Requests Policy under regular review and we will place any updates on the Tidenham Parish Council website.

3. **Contact Details**

   Please contact us if you have any questions about this Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

   The Data Controller, Tidenham Parish Council, Wood Cottage, Clanna, Alvington, Glos GL15 6AJ Email: clerk@tidenhamparishcouncil.co.uk

   Adopted by Full Council 20th June 2018 Minute 2018/2019 Page 5 Item 15 (d)

   To be reviewed June 2019

[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.