Yateley Town Council Subject Access Request Policy 2020

Yateley Town Council will promote this policy via its website www.yateley-tc.gov.uk.

1. **Upon receipt of a SAR Yateley Town Council will:**
   (a) Verify whether we are controller of the data subject's personal data. If we are not a controller, but merely a processor, we will inform the data subject and refer them to the actual controller;
   (b) We will verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject as detailed below;
   (c) We will verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not, we will request additional information;
   (d) We will verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, we may refuse to act on the request or charge a reasonable fee;
   (e) We will promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR;
   (f) We will verify whether we process the data requested. If we do not process any data, we will inform the data subject accordingly. At all times we will make sure the internal SAR policy is followed and progress can be monitored;
   (g) We will ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted;
   (h) We will 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, we will ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. **Responding to a SAR**
   (a) We will 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, we will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

   (b) We will 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 will 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

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

(d) If data on the data subject is processed, we will 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;

(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;

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

[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.

3. A database will be maintained to allow the Council to report on the volume of requests and compliance against the statutory timescale.

4. All letters will 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) There 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.

Amendment Record

Version 1: Approved by Finance & Policy Committee 04.06.18
Version 2: Approved by Finance & Policy Committee 09.09.19
Version 3: Approved by Finance & Policy Committee 07.09.20

[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 organisations head quarters 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.