

DRAUGHTON PARISH COUNCIL

DATA PROTECTION ACT

Subject Access Policy

To facilitate **Subject Access Requests (“SARs”)**, the Council will:

- A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).
- B. Implement an SAR policy within the council, including internal procedures, which specify responsibilities for the accurate and timely handling of SARs, including requests for rectification, erasure or restriction of processing.
- C. Ensure 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.
- D. Where possible, implement standards to respond to SARs, including a standard response.

1. Upon receipt of a SAR, the 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) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- (c) Verify 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 we process the data requested. If we 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.

2. Responding to a SAR - the Council will:

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

- (c) If data on the data subject is processed, the following information will be included as a minimum 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 Rules¹ or EU model clauses²;
 - (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.
- (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 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.

Notes:

1. We 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. We 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*
 - 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
2. Depending on the degree to which personal data is organised and structured, we 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 we are responsible for or own.
3. We must not withhold personal data because we believe it will be misunderstood; instead, we should provide an explanation with the personal data. We 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. We may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. We must redact any exempt personal data from the released documents and explain why that personal data is being withheld.
4. We will make these procedures clear on forms and on the council website
5. We will promulgate procedures through the use of induction, performance monitoring and training, as well as through establishing and maintaining appropriate day to day working practices.
6. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.
7. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.