GREAT GADDESDEN PARISH COUNCIL - DATA PROTECTION POLICY

To be reviewed May 2020

1. Policy, scope and objectives

1.1 The Parish Council is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information we collect in accordance with the General Data Protection Regulation (GDPR), including: -

a. processing personal information only where this is strictly necessary for legitimate l purposes;
b. collecting only the minimum personal information required for these purposes
c. providing clear information to individuals about how their personal information will be used and by whom;
d. only processing relevant personal information;
e. processing personal information fairly and lawfully;
f. maintaining an inventory of the categories of personal information processed by the Council;
g. keeping personal information accurate and, where necessary, up to date;
h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate purposes;
i. respecting individuals' rights in relation to their personal information, including their right of subject access;
j. keeping all personal information secure;
k. only transferring personal information outside the EU in circumstances where it can be adequately protected;
l. the application of the various exemptions allowable by data protection legislation;

1.2 The Parish Council has registered with the Information Commissioner (ICO) recognizing it is a data controller and that the Council processes certain information about data subjects. The Parish Council has identified all the personal data that it processes and this is contained in the Data Register.

1.3 A copy of the ICO notification details is retained by the Clerk

1.4 The Clerk is responsible, each year, for reviewing the details of notification, in the light of any changes to the Council's activities (as determined by changes to the Data Register)

The policy applies to all Employees and Councillors and interested parties of the Council such as outsourced suppliers. Any breach of the GDPR will be dealt with under the Council's disciplinary policy and may be a criminal offence, in which case the matter must be reported as soon as possible to the appropriate authorities.

No third party may access personal data held by the Council without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which the Council is committed, and which gives the Council the right to audit compliance with the agreement.

2. Definitions used by the organisation (drawn from the GDPR)

Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behavior to data subjects who are resident in the EU.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3. Responsibilities under the General Data Protection Regulation

3.1 The Council is a data controller and data processor under the GDPR.
3.2 The Clerk and Councillors are responsible for developing and encouraging good information handling practices within the Council;
3.3 Staff are responsible for ensuring that any personal data supplied by them, and that is about them, is accurate and up-to-date.

4. Risk Assessment

Allied to the general Risk Assessments carried out by the Council, the purpose is to ensure that the Council is aware of any risks associated with the processing of particular types of personal information.

The Council shall manage any risks, which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Prior to implementation of any changes made to the way the Council conducts its business The Clerk shall in conjunction with the Councillors, review GDPR principles to ensure there is no added risk in making the change.

Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level.

5. Data protection principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and the Council's policies and procedures are designed to ensure compliance with them.

5.1 Personal data must be processed lawfully, fairly and transparently.

GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms".

Information must be communicated to the data subject in an intelligible form using clear and plain language. The specific information that must be provided to the data subject must as a minimum include:

- the contact details of the Clerk;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;

- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

5.2 Personal data can only be collected for specified, explicit and legitimate purposes.
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the Council's GDPR registration.

5.3 Personal data must be adequate, relevant and limited to what is necessary for processing.

- The Data Protection Officer is the GDPR Owner and is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Clerk.
- The Clerk will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by the Council's documented procedures, the holder of the data is responsible for ensuring that it is securely deleted or destroyed in line with the Council's policy for disposal of storage media.

5.4 Personal data must be accurate and kept up to date.

- Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- The Council are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by the Council is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.
- Staff should notify the Council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- Where personal data is retained beyond the processing date, it will be [minimised/encrypted/pseudonymised] in order to protect the identity of the data subject in the event of a data breach.
- Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

5.6 Personal data must be processed in a manner that ensures its security

5.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

5.8 Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

5.9 Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

6. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.
  Data subjects may make data access requests as described in the our subject access request procedure this procedure also describes how the Council will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

Data Subjects who wish to complain to the Council about how their personal information has been processed may lodge their complaint directly with the Clerk.
Data subjects may also complain directly to the ICO.

7. Consent

The Council understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

8. Security of data

All Employees are responsible for ensuring that any personal data, which the Council holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Council to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, Personal data will be kept:

- in a locked drawer or filing cabinet; and/or
- if computerised, password protected and/or
- Stored on computer media, which are encrypted.

Manual records may not be left where they can be accessed by unauthorised personnel. As soon as manual records are no longer required for day-to-day use, they will be destroyed.

Personal data may only be deleted or disposed of in line with the Document Retention and Security Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

9. Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the Council in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Council, and information obtained from third-party organisations about that person. Subject Access Requests are dealt with as described in the Appendix 1 to this policy.

10. Disclosure of data

The Council will ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Council's business.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Clerk.

APPENDIX 1

Subject Access Request Procedure

1. Scope

All personal data processed by the Council is within the scope of this procedure.

Data subjects are entitled to ask:

- Whether the Council is processing any personal data about that individual and, if so, to be given:
  - a description of the personal data;
  - the purposes for which it is being processed; and,
  - details of who will be allowed to see the personal data.

- To be provided with a copy of the information and to be told about the sources from which the Council derived the information.

2. Responsibilities

The Clerk is responsible for the application and effective working of this procedure, and for reporting to the Council on Subject Access Requests (SARs).

3. Procedure

3.1 Subject Access Requests must be made to the Council in writing and be clear and unambiguous.

3.2 The data subject must provide evidence as to their identity, in the form of a current passport/driving license, and the signature on the identity must be crosschecked to that on the SAR.

3.3 The data subject must identify the data that is being requested and where it is being held and this information must be shown on the SAR request. Note that the data subject is entitled to ask for all data that the firm holds, without specifying that data.

3.4 The date by which the identification checks have been completed and that the specification of the data sought is clear must be recorded; The Council has one month from this date to provide the requested information. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

3.5 The SAR request is immediately forwarded to the Clerk who will ensure that the requested data is collected within the time period.

Collection will entail either:

- Collecting the data specified by the data subject, or

- Searching all databases and all relevant filing systems (manual files) in the Council, including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives.

3.6 The Clerk will maintain a record of requests for data.

3.7 The Clerk is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

3.8 If the requested data falls under one of the following exemptions, it does not have to be provided:

- Crime prevention and detection.
- Negotiations with the requester.
- Management forecasts.
- Confidential references given by the Council (not ones given to the Council).
- Information used for research, historical or statistical purposes.
- Information covered by legal professional privilege.

3.9 The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

APPENDIX 2

Personal Data Breach Notification Procedure

1. **Scope**

This procedure applies in the event of a personal data breach under Article 33 *Notification of a personal data breach to the supervisory authority,* and Article 34 *Communication of a personal data breach to the data subject* of the GDPR.

2. Responsibility

All users of personal data at the Council (whether Employees, contractors or temporary Employees and third-party users) are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. Procedure – Breach Notification Data Processor to Data Controller

All shall report any personal data breach to the Clerk. The Clerk will record the breach. Confirmation of receipt of this breach information is made by email.

4. Procedure – Breach Notification Data Controller to Supervisory Authority

The Clerk will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. If a risk to the aforementioned is likely, the Clerk will report the personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The following information will be provided to the supervisory authority:

- A description of the nature of the breach
- The categories of personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Name and contact details of the person responsible within the firm
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation
- The information relating to the data breach, which may be provided in phases.

5. Procedure – Breach Notification Data Controller to Data Subject

Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject the Clerk shall notify the affected data subjects without undue delay.

The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified above.