GREAT GLEMHAM PARISH COUNCIL
DATA PROTECTION POLICY

This policy has been created to ensure that all the Council's policies relating to data protection, collection, use, management and storage are in one single document that covers the following risk areas:

- Data Protection
- Data Security
- Data Retention
- Breach Reporting

A separate section is devoted to each subject which provides relevant guidelines as well as the policies themselves.

Data Protection

It is the Council's policy to treat all stakeholders (data subjects) fairly and lawfully when processing, storing and sharing their personal data and, in doing so, to capture the minimum amount of information to do this effectively.

The Council is registered with the Information Commissioners Office (ICO). Its registration number is Z7456521 and registration is renewable every year on 12TH March. Details can be viewed in the public record via the following link https://ico.org.uk/esdwebpages/search

In addition, the Council ensures that its registration details remain up to date and any change is notified to the Information Commissioner's Office no later than within 28 days of any change occurring.

The Council treats all personal information as private and confidential and it will not release information to anyone else except where:

- the data subject gives explicit, unambiguous consent
- to do so is a legal requirement

Data held will, at all times, be processed and stored securely within the requirements of data protection laws and in accordance with the Council's data security policy.

Governance of Data Use

Privacy by design is an implicit requirement of data protection and the Council has a general obligation to implement technical and organisational measures to show that it has considered and integrated data protection into its processing activities.

The Council understands the importance of having robust governance, systems and controls in place to protect the rights of data subjects and to ensure its on-going compliance with the requirements of data protection law.

The Parish Clerk (Caroline Emeny) has primary responsibility for data protection, ensuring that compliance with the regulations is central to the culture within the Council and that all Councillors and staff are discharging their duties appropriately with regard to personal data. Also, that the Council's Privacy Notice remains accurate and up to date and that it maintains an archive of all Privacy Notices issued.

Legal Basis for Processing Personal Data

The Council ensures that at all times, it is able to process, store and share personally-identifiable information legally.

Personally-Identifiable Information is:

- Any information relating to a living person that can be used to directly or indirectly identify that person
- Full name, email address, date of birth, IP address / website cookies
- Purchases, downloads, subscriptions and services used
- Questions and responses, promotions used, survey responses
- Financial history, banking/credit, payment transactions and donations
- Healthcare and education services used
- CCTV recordings, gender identity, location data, credit card data
- Judgments/sanctions, government services
- Capable of identifying an individual either on its own or when combined with other information
- Internal account numbers, PINs and passwords, IMEIs, National Insurance number
- Driving licence number, passport number

Special Category or High Risk Data is:

- Race/ethnic origin, political opinions, religious beliefs and union membership
- Biometric, genetic, health and medical data
- Information relating to sexual orientation or sex life
- Details of criminal convictions

Consent

Consent for Data Processing

In all other situations, it is Council policy that processing consent must be freely given, unambiguous and on an opt-in, not opt-out, basis. In such other situations, consent will not be a condition of provision of service.

The Council will ensure that consent for the use of personal data is obtained specifically for each of purpose and separately from consent to any other terms or conditions.

Privacy Notices

When requested, all data subjects will be provided with a copy of, or access to, the Council's Privacy Notice. This will be retained in an archive of version-controlled Privacy Notices.

In order to demonstrate compliance with the requirements for consent, when consent is given by a data subject, the Council's system will record the following:

- Name of data subject providing consent
- Date consent obtained
- Method of consent (verbal, E-Mail etc)

Data Sharing

The Council acknowledges that it will be necessary to share personally-identifiable information (including special category data, where relevant) with third parties (acting as data processors) in order to facilitate and assist with the following relationships:

- Fulfilment of its public duties
- Employment of personnel
- Sourcing services from third parties
- Providing services to the local community

The Council will take proportionate steps to ensure that all third parties receiving data from it are also compliant with data protection requirements.

The Council recognises that a failure of any data processor to comply with their legal requirements will have a direct impact on its ability to demonstrate compliance.

Data Breaches

Data protection law obliges Councils to notify the ICO of a breach which is likely to result in a risk to the rights and freedoms of any data subject. This is defined as something which, if unaddressed, is likely to have a significant detrimental effect on individuals, for example, to result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of data subjects, the Council will notify the data subject concerned directly.

Data Security

Risk Assessment

The Council has carried out a security risk assessment. Following this assessment it has:

- Adopted data loss and breach notification procedures to ensure compliance with legal and regulatory obligations.
- Given due consideration to how data will be segregated (when using a public cloud)
- Taken appropriate steps to mitigate security risks so that its overall security exposure is acceptable.
- Considered the sensitivity of data and how data is transmitted, stored and where necessary, encrypted.

The Council currently utilises the following system and network security measures:

- Password encrypted standalone laptop
- Anti Virus and Fire Wall protected internet security
- Data backup via a separate hard drive
- Support for all firewalls, routers, wireless configuration
- Supported user platforms and Windows and Smartphone operating systems

Data Retention

The Council recognises that data protection law requires it to hold data for no longer than is absolutely necessary. Data is therefore stored in line with the following principles.

Once the compulsory retention period has passed, data will be destroyed and deleted securely.

In order to achieve this, the Council has instigated a process to identify data due for deletion and its destruction and removal from its systems followed by secure shredding of manual documentation and deletion of data from computer systems by the Council's members and staff.

Rights of Data Subjects

The Council recognises the rights of data subjects and these are respected at all times.

Any request from a data subject to access their data, refuse to provide it or have any data supplied rectified, erased or restricted will be actioned taking into account the Council's legal and regulatory obligations.

Where a data subject wishes to exercise their right of access or rectification, this will be acted upon promptly but in all cases, no later than 30 days from the date of request. No charge will be make for providing the data subject with the information or the correction of any incorrect or inaccurate information we hold.

In terms of data retention, such response will also be compliant with requirements specified by the Financial Conduct Authority and in the Companies Act or other legislation.

Appendix 1 - Data Breach Reporting Form

Data Protection Breach Record

The following headings provide a basis for a Council to record details of any breach of the Data Protection Act 2018 for internal purposes. Where necessary, a breach must be reported to the ICO within 72 hours: see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

1. Date of incident.

2. Details of the data protection breach – how did it happen and why?

3. Nature of the personal data at risk – indicate if any special category or financial data is affected.

4. The data of how many individuals has been (potentially or otherwise) compromised

5. What are the potential consequences for those individuals?

6. If necessary, have the data subjects been informed?

7. Is notification to ICO and/or police required?

8. Date(s) of notifications, if applicable.

9. Reason for any delays between breach identification and notification.

10. Have any data subjects complained to the Council about the incident?

11. Has the Council taken any action to minimise /mitigate the effect on the affected individuals? If so, include details.

12. Has the data placed at risk now been recovered or protected? If so, provide details of how and when this occurred.

13. What steps has the Council taken to prevent a recurrence of this incident?

14. Does the Council need to provide any detailed guidance to members and staff on the handling of personal data in relation to this incident?

Once the above information has been obtained, but in all cases not longer than 72 hours from the date of awareness of the breach, notification of the breach will be made by the Parish Clerk to the ICO, and if appropriate, to the data subject.