Great Gonerby Parish Council

Data protection policy

1. Great Gonerby Parish Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulate the use of personal data. This is data that can be linked to an individual data; it could be a name, address, date of birth, telephone number or email address.

2. **GDPR overview**. The GDPR set out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about another person, whether electronically or on paper. The Parish Council must notify the Information Commissioner that it holds personal data about individuals and of any changes to the data or how it is managed.

3. When dealing with personal data, the Parish Council staff and councillors must ensure that it is:

a. **Used transparently**. The Parish Council recognises its responsibility to be open and honest with people when taking personal details from them: they will be clear as to why they want a particular piece of personal information.

b. **Specific to need.** Data must only be collected for specific, explicit and legitimate purposes only.

c. **Relevant.** Data will be monitored so that only that which is needed is held.

d. **Accurate and current.** Personal data should be accurate; if it is not, then it should be corrected. Data no longer needed should be shredded or securely disposed of.

e. **Accessible to the subject.** The Parish Council is aware that people have the right to access any personal information that is held about them. To obtain this information about themselves an individual must submit a Subject Access Request (SAR) in writing to the Parish Clerk: this can be done in hard copy, email or through social media. The process for SARs is detailed in a separate policy.

f. **SAR responses**. A SAR response must be sent within 30 days of receiving the SAR, be free of charge and include all the personal information held about an individual. This includes: how and to what purpose the personal data is processed, how long the data will be required for and who has access to the data.

(1) If a SAR response includes personal data of other individuals, the Parish Council must not disclose this to the requester. That personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the requester.

(2) Individuals have the right to: have their data rectified if it is incorrect, have their data erased, have processing of the data restricted and object to the storage or processing of their data.

g. **Kept securely.** Data should be protected against unauthorised or unlawful access or processing and against accidental loss, destruction or damage.

4. **Data storage**. The Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely locked in a filing cabinet in the Parish Council Office so will not be available for public access. All data stored on the Parish Council computer is password protected.

5. **Data deletion**. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of the Parish Council's document retention policy, it will be shredded or securely deleted from the computer.

6. **Confidentiality**. The Parish Council staff and councillors must be aware that when complaints or queries are made, these must remain confidential unless the subject gives permission otherwise. A signed and dated document, giving permission to release information by the subject, should be kept on file for future reference. The handling of personal data must also remain confidential.