Great Missenden Parish Council
Data Protection Policy

Great Missenden Parish Council has committed itself to implement and abide by the General Data Protection Regulations (GDPR), effective 25 May 2018.

Definition of terms

- **Personal data** is just about any fact about a person, down to the level of phone number. Some facts, e.g. ethnicity or religion are identified as "sensitive" requiring extra care.
- **Data processing** is doing just about anything with personal data – collecting, using, storing, passing on and (N.B.) deleting it.
- **A data controller** is a person or body, in this case the Parish Council, who says how personal data is treated
- **Data processors**, in this case mainly the Parish Clerks, are people who process data.

The Council's Duties and Commitments

- Wherever possible, to obtain specific and informed consent for the processing of personal data, and to do nothing with such data for which we do not have consent or another legal reason for processing. However, that consent becomes a secondary consideration when there is a statutory reason for processing it or we have a "legitimate interest" reason for processing, i.e. that we cannot function as a Parish Council without so doing.
- To retain personal data only for so long as there is a justification.
- To make all reasonable attempts to keep all personal data we hold secure.
- To publicise and implement the rights of persons whose data we hold
  - to know what data we hold and why
  - to correct any errors in the data
  - to demand that we erase it if this is legally permissible and we do not need to retain it for our legitimate interest to operate as a Parish Council
  - to know what we have done with it
  - to be informed of any breaches of data protection and to have any such breaches properly addressed.

Data Security

- Primarily, personal data is held within the Parish Office. Except as below, security depends upon the security of this office. It is deemed to have an acceptable level of physical security. It has an alarm system.
- Personal data is held within GDPR compliant cloud storage (Microsoft). Passwords are complex and known only to the Clerks.
- All the parish council's owned laptops are protected by firewall, anti-virus and anti malware software, which is and will be kept up to date. A professional review of our cyber security has been conducted.
- Data backup is included with Microsoft cloud storage account. However, six monthly external hard drive back ups are made and retained for 2 years. These are kept in a fire safe whose keys are held by the clerks alone.

Email Policy

- The Clerks and councillors are directed to bear in mind data protection issues whenever sending emails.
- Email addresses are considered personal data. Wherever possible we will avoid writing or forwarding emails with open recipient lists where the council does not have permission to disclose addresses of such recipients. (All councillors will be deemed to have given consent to be on open distribution lists to other councillors.)
- Councillors are required to consider the GDPR when forwarding or otherwise using council emails.

Disposal of Data

The GDPR requires that data be not retained for longer than necessary, no if its owner demands its deletion and this is permitted.

- The Clerks are required to delete any data for which a legal deletion demand is made and no over-riding reason for retention exists, or for which there is clearly no justification for retention.
- Deleted data may remain on the backups until backup recycling destroys it. This is deemed acceptable but
    - No data that has been deleted may be recovered from backups and use made of it
    - In the event that backups must be used to restore data (after a data loss), and data that has been deleted must be deleted from the restored set.

Communications to the Council

If a member of the public writes or sends an email to us (to the Council, to the Clerks or to an individual Councillor) it is usual for what is sent to be distributed to all Councillors and to be discussed in Council Meeting, which is in public. As a general rule, we will assume that, by writing, the writer has given permission for this (and to use their address data for any reply). The name and contact details will be redacted in copies distributed to Councillors unless the writer has given permission for this information to be shared or there is a strong and legal reason for including it. An indication of the writer's geographical area or street may be appended should this be judged relevant. If our Clerks deem that the issue is sensitive, they may contact the writer and ask for specific permission to use the communication in this way.

Councillor Surgeries

If and when surgeries are held, all members of the public who visit councillor surgeries will be told what use will be made of any information they give us, and asked for consent to this. No more of this data will be disseminated than is necessary. Written notes will only be taken after gaining consent to do so. Privacy notices will be available and handed out if deemed appropriate. (It is to be note that GDPR strictly covers only data that is processed electronically or kept in a filing system.)

Cemetery Data

A particular difficulty might have been thought to exist in respect of certain very old data, particular related to cemeteries, generated before the 1988 act, let alone before the GPDR. This is held in both paper and electronic form. Obtaining consent to retain these would sometimes be impracticable, in all cases unreasonably onerous. Processing of this data is justified by The Local Authorities Cemeteries Order 1977 and thus does not need consent.

Address Book

As with archival data, obtaining consent to retain all address book entries will sometimes be impracticable, in all cases unreasonably onerous, and in any event is likely to involve using (processing) the very data for which permission to process is sought. Processing (by retaining and if appropriate using) this data will be covered by the legitimate interest justification. However:

- Efforts will be made to purge any address book entries for which there is no identifiable reason for retention.
- Whenever a new entry is made, efforts will be made to check that we have informed consent and/or a justification to do so.
- Whenever an entry is used, efforts will be made to check that we already have informed consent and/or a justification to do so, and of not to obtain such consent.

Breaches of the Regulations

Please see Data Breach Handling Policy which is to be implemented if a breach is detected or complained about.

Review

This policy and associated documents are to be reviewed annually, ideally at the same time as the Council's Standing Orders are reviewed or on the anniversary of GDPR coming into law. Also, any councillor can call for a review at any time if a possible need for a change is identified.

Data Protection Officer

Parish Councils are not required Data Protection act 2018 to appoint a DPO. GMPC has decided not to do so, but to reconsider this decision in the event of a serious data breach or complaint.

Date adopted: 05.05.18
Date of review: 08.04.19

Date of review: May 2020

Date of review: May 2021

Date of review: May 2022

Date of review: May 2023

Date of review: May 2024

Date of review: May 2025