# Data Protection Policy

**Scope of the Policy**
This policy applies to the work of the Burton Pedwardine Parish Meeting. The policy sets out the requirements that the Meeting has for personal information for: Meeting management purposes, the delivery of information to electors and the wider public and when processing personal data on behalf other organisations. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the Clerk to ensure that the Meeting is compliant. This policy should be read in tandem with the Meeting's Privacy Policy.

**Terms used in this Policy**

| | |
|---|---|
| Administrator | A specified member of the Meeting (the Clerk by default). |
| Clerk | An elected member of the Meeting responsible for administration. |
| Contractor | A commercial organisation contracted to maintain and support parts of the System including email and website under direction of the Administrator. |
| Data Controller | A person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data are, or are to be, processed. |
| Data subject | An individual who is the subject of personal data. |
| Members | Electors of the Parish and entitled to participate in the Meeting. |
| Meeting | The Burton Pedwardine Parish Meeting. |
| Service | The delivery of information to Members about the Meeting, parish activities or Local Government. |
| System | Any IT system or hardware used or provided for data storage and support services and materials. |

**Purpose**
This data protection policy ensures that the Meeting:

- Complies with data protection law and follows good practice.
- Protects the rights of data subjects.
- Is open about how it stores and processes personal data.
- Protects itself from the risks of a data breach.

**Data Protection Principles**
The General Data Protection Regulation identifies 8 data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner.
Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot 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 individuals in relation to the processing of personal data.

**Lawful, Fair and Transparent Data Processing**
The Meeting's lawful basis for processing is:

- Legitimate interests: for personal data processed to provide the information to the Meeting. A Legitimate Interests Assessment has been conducted and shall be reviewed annually or when circumstances change.

In providing information to the Meeting, the Clerk sometimes requests personal contact information from data subjects for communicating about their involvement with the Meeting. Forms used to request personal information will contain a privacy statement informing data subjects why the information is being requested and what the information will be used for. If a data subject requests not to receive certain communications this will be acted upon promptly.

**Processed for Specified, Explicit and Legitimate Purposes**
Data subjects shall be informed as to how their information will be used and the Clerk shall seek to ensure that data is not used inappropriately. Appropriate use of information provided by Members will include:

- Communicating with Members about the Meeting's events, activities and management of work.
- Communicating with Members about the Meeting's policies, events and activities.
- Communicating with Contractors about specific issues that may arise during the course of providing information via the System.

The Administrator shall ensure that Members are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending Members marketing and/or promotional materials from external service providers.

The Administrator shall ensure that all data subjects' information is managed in such a way as to not infringe an individual members rights which include:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

**Adequate, Relevant and Limited Data Processing**
Data subjects will only be asked to provide information that is relevant the delivery of the Beacon Service. This will include:

- Name.
- Address.
- Email address.
- Telephone number.

Where additional information may be required, such as health-related information, this will be obtained only from the data subjects who will be informed as to why this information is required and the purpose that it will be used for.

There may be occasional instances where a data subject's data needs to be shared with a third party due to an accident or incident involving statutory authorities, or where it is in the best interests of the data subject, or in those instances where the Meeting has a substantiated concern.

Data subjects' contact details shall be deleted no longer than two years after the data subject ceases to have involvement with the Meeting.

**Accuracy of Data and Keeping Data up to Date**
The Administrator has a responsibility to ensure data subjects' information is kept up to date. Data subjects' information shall be reviewed and validated at least annually or when policy is changed. Data subjects are informed to let the Administrator know if any of their personal information changes.

**Subject Access Request**
Data subjects are entitled to request access to the information that is held about them by the Meeting. The request needs to be received in the form of a written request to the Administrator. On receipt of the request, the request will be formally acknowledged and dealt with within 14 days unless there are exceptional circumstances as to why the request cannot be granted. The Administrator will provide a written response detailing all information held on the member. A record shall be kept of the date of the request and the date of the response.

**Accountability and Governance**
The Administrator is responsible for ensuring that the Meeting remains compliant with data protection requirements and can evidence that it has.
The Administrator shall ensure that new Members involved in Meeting administration receive an induction into how data protection is managed within the Meeting. All such Meeting administrators shall confirm agreement with this policy annually. The Administrator shall review what data is held, its protection and manage/record who has access to it. The Administrator shall also stay up to date with Data Protection guidance and practice within the Local Government.

**Secure Processing**
The Administrator is the Data Controller and has responsibility to ensure that data is both securely held and processed. Data handling shall follow documented processes. These will include but are not limited to:

- Members using strong passwords.
- Members not sharing passwords.
- Restricting access of sharing member information to those involved in Meting administration who need to communicate with data subjects on a regular basis.
- Using password protection on laptops and PCs that contain or access personal information.
- Using password protection or secure cloud systems when sharing data between Meeting administrators.
- Ensuring firewall security on Meeting administrators' laptops or other devices.

**Service Providers**
The Administrator has scrutinised the Terms and Conditions of each Contractor listed below and judged that they are GDPR compliant.

| Contractor | Terms Reviewed | Judged GDPR Compliant (Y/N) | Used for Member data |
|---|---|---|---|
| HugoFox | 30 Dec 2025 | Y | Y |
| Parish Online | 30 Nov 2025 | Y | Y |
| Survey Monkey | 20 Mar 2026 | Y | Y |
| Mailchimp | 22 Mar 2026 | Y | Y |
| Trello | 22 Mar 2026 | N - Not to be used | |
| WhatsApp | 22 Mar 2026 | N - Not to be used | |

**Data Breach Notification**

Were a data breach to occur action shall be taken to minimise the harm by ensuring all data subjects are aware that a breach had taken place and how the breach had occurred. The Administrator shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. A discussion would take place between the Administrator and the Meeting Chair as to the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified. The Administrator shall also contact the relevant data subjects to inform them of the data breach and actions taken to resolve the breach.

If a data subject contacts the Administrator to say that they feel that there has been a breach by the Meeting or its Contractors, the Administrator shall ask them to provide an outline of their concerns. If the initial contact is by telephone, Administrator will ask them to follow this up with an email or a letter detailing their concern. The concern will then be investigated by Meeting members who are not in any way implicated in the breach. Where the Meeting needs support or if the breach is serious, an Extraordinary Parish Meeting may be called. Breach matters will be subject to a full investigation; records will be kept and all those involved notified of the outcome.

**Version control and amendment history**

| Date approved | Version Number | Revision / amendments made | Review date |
|---|---|---|---|
| | V0a | Draft | Apr 2026 |
| | | | |