

Monday 12th August 2019

Data Protection Policy (GDPR)

Scope of the policy

This policy applies to the work of the Better Wetherby Partnership (BWP). It sets out the requirements that the BWP has to gather information for membership and campaigning purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation (GDPR). The policy is reviewed on an ongoing basis by the BWP Steering Group to ensure compliance. It should be read in conjunction with the Privacy Policy of the BWP.

Why this policy exists

This data protection policy ensures that BWP:

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

General guidelines for Steering Group members, Sub-Group members and nominated Administrators

1. The only people able to access data covered by this policy should be those who need to communicate with or provide a service to members and supporters.
2. BWP will provide appropriate induction training to Steering Group members, Sub-Group members and nominated Administrators to help them understand their responsibilities when handling data.
3. Steering Group members, Sub-Group members and nominated Administrators should keep all data secure, by taking sensible precautions and following the guidelines below.
4. Strong passwords must be used and they should never be shared.
5. Data should not be shared outside of the BWP unless with prior consent and/or for specific and agreed reasons.
6. Member and supporter information should be reviewed periodically to ensure accuracy.

Data protection principles

The General Data Protection Regulation identifies key data protection principles:

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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, having regard to the purposes for which they are processed, are erased or rectified without delay;

Principle 5 – Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for the which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest , scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Principle 6 - 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.

Lawful, fair and transparent data processing

BWP requests personal information from potential members and supporters and for sending communications about their involvement with the organisation. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. The lawful basis for obtaining member information is due to the contractual relationship that the BWP has with individual members. In addition, members will be asked to provide consent for specific processing purposes. BWP members will be informed as to who they need to contact should they wish their data not to be used for specific purposes for which they have provided consent. Where these requests are received, they will be acted upon promptly and the member will be informed as to when the action has been taken.

Processed for specified, explicit and legitimate purposes

Members will be informed as to how their information will be used and the Steering Group will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members and supporters and sending information about BWP events and activities.
- Communicating with members and supporters about specific issues that may have arisen.

The BWP Steering Group will ensure that Sub-Group members and Administrators are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending BWP members and supporters marketing and/or promotional materials from external service providers.

BWP will ensure that members' and supporters' information is managed in such a way as to not infringe their individual 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 object

Adequate, relevant and limited data processing

Members of the BWP will only be asked to provide information that is relevant for membership or supporter purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number

Photographs

Photographs are classified as personal data. Where group photographs are being taken, members should step out of shot if they do not wish to be in the photograph.

Accuracy of data and keeping data up-to-date

BWP has a responsibility to ensure members' and supporters' information is kept up to date. Members and supporters are requested to inform the Steering Group Secretary of any personal information changes.

Accountability and governance

The BWP Steering Group is responsible for ensuring that the BWP remains compliant with data protection requirements and can evidence that it has. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely. The BWP Steering Group will ensure that new members joining the Steering Group or one of the Sub-Groups, receive an induction into the requirements of GDPR and the implications for their role. They will also ensure that Administrators are made aware of their responsibilities in relation to the data they hold and process. The Steering Group will review data protection and who has access to information on a regular basis as well as reviewing what data is held. When Steering Group Members, Sub-Group members and Administrators relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Secure Processing

Steering Group and Sub-Group members and Administrators have a responsibility to ensure that data is both securely held and processed. This will include:

- Steering and Sub-Group members and Administrators using strong passwords
- Steering and Sub-Group members and Administrators not sharing passwords
- Restricting access of member information to those Steering Group members, Sub-Group members and nominated Administrators who need to communicate with members on a regular basis
- Using password protection on laptops and PCs that contain personal information
- Using password protection or secure cloud systems when sharing data between Steering and Sub-Group members and Administrators
- Ensuring firewall security is on the laptops or other devices of Steering and Sub-Group members and Administrators.

Subject Access Request

BWP members and supporters are entitled to request access to the information that is held on them by BWP. This should take the form of a written request to the Secretary of the BWP. On receipt, the request will be formally acknowledged and dealt within 30 days. A written response detailing all information held on the member will be provided. A record shall be kept of the date of the request and the date of the response.

Data Breach Notification

Were a data breach to occur, action shall be taken to minimise the harm. This will include ensuring that all Steering Group members are made aware that a breach has taken place and how the breach occurred. The Steering Group shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Steering Group will determine the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified. The Steering Group shall also contact the relevant BWP members and supporters to inform them of the data breach and actions taken to resolve the breach.

Where a BWP member or supporter feels that there has been a breach by the BWP, a Steering Group member will ask the member to provide an outline of the breach. If the initial contact is by telephone, the Steering Group member will ask the BWP member to follow this up with an email or a letter detailing their concern. The alleged breach will then be investigated by members of the Steering Group who are not in any way implicated in the breach. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy Review

This policy was adopted at a meeting of the Better Wetherby Partnership Steering Group on 12th August 2019.

It will be reviewed on an ongoing basis and at least every 2 years.