

# Midhurst Green Volunteers



## Data Protection Policy

Midhurst Green Volunteers (MGV) may collect and use certain types of personal information about volunteers and other individuals who come into contact with the group. It may be required by law to collect and use certain types of information to comply with statutory obligations and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation. GDPR applies to all computerised data and manual files if they come within the definition of a filing system.

Personal data is information that identifies an individual. A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to e.g. a person's political beliefs, ethnicity etc.

MGV does not intend to seek or hold sensitive personal data except where it has been notified of the information, or it comes to light via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.

MGV will take reasonable steps to ensure that volunteers will only have access to personal data where it is necessary for them to carry out their duties. MGV will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

### Disclosure of Personal data to Third Parties

The following list includes the most usual reasons that MGV will authorise disclosure of personal data to a third party:

- to give a confidential reference relating to a current or former volunteer;
- for the prevention or detection of crime;
- for the assessment of any tax or duty;
- where it is necessary to exercise a right or obligation conferred or imposed by law;
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice;

All requests for the disclosure of personal data must be sent to the Chairman, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

### Rights of Individuals

An individual has the right to object to the processing of their personal data and to block or suppress the processing.

Where such an objection is made, it must be sent to the Chairman who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

An individual has the right to request the rectification of inaccurate data or incomplete data without undue delay. Where any request for rectification is received, it should be sent to the Chairman and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable.

Should there be a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual who may appeal to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data.

Individuals have a right, in certain circumstances e.g. when personal data is no longer necessary, to have data permanently erased without undue delay.

The Chairman will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

### Breach Of Any Requirement Of The GDPR

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Chairman.

Once notified, the Chairman shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Chairman concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having been reported to MG.V.

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries;
- the likely consequences of the breach;
- the measures proposed or already taken to address the breach

If the breach is likely to result in a high risk to the affected individuals then the Chairman shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

The Chairman shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Charity and a decision made about implementation of those recommendations

**Signed .....** **Chairman**

**Dated:.....**

**Date of Review:.....**