VPA *THE HOLMER GREEN GARDENING ASSOCIATION*
founded in 1944

DATA PROTECTION POLICY

Scope of the policy

This policy applies to the operations of VPA, The Holmer Green Gardening Association (hereafter 'the VPA'). The policy sets out the requirements that the VPA has in order to gather personal information for membership 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. The policy is reviewed on an ongoing basis by the VPA Committee Members to ensure that the VPA is compliant. This policy should be read in tandem with the VPA's Privacy Policy.

Why this policy exists

This data protection policy ensures that the VPA:

- complies with data protection law and follows good practice
- protects the rights of members
- is open about how it stores and processes members' data
- protects itself from the risks of a data breach.

General guidelines for Committee Members

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to the members of the VPA
- Data should not be shared informally or outside of the VPA
- The VPA will, if required, provide induction training to Committee Members to help them understand their responsibilities when handling personal data
- Committee Members should keep all data secure, by taking sensible precautions and following the guidelines below
- Strong passwords must be used and they should never be shared
- Personal data should not be shared outside of the VPA unless with prior written consent and/or for specific and agreed reasons
- Member information should be reviewed and consent refreshed periodically via the membership renewal process or when policy is changed.

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.

© Holmer Green VPA, 2026

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 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.

Some of these principles are explored in more detail in the sections that follow.

Lawful, fair and transparent data processing

The VPA requests personal information from potential members and members for the purpose of sending communications about their involvement with the VPA. 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. Members will be asked to provide consent for their data to be held and a record of this consent along with member information will be securely held. VPA members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a VPA member requests not to receive certain communications this 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 Committee of the VPA will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about the VPA's events and activities, including via the bi-monthly VPA newsletter and via email

 © Holmer Green VPA, 2026

- Communicating with members about their membership and/or renewal of their membership.
- Communicating with members about specific issues that may have arisen during the course of their membership.

The VPA will ensure that members' 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

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

- Name
- Postal address
- Email address
- Telephone number.

Where additional information may be required, such as health-related information, this will be obtained with the specific consent of the member who will be informed as to why this information is required and the purpose for which it will be used.

There may be occasional instances where a member's data needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the member or the VPA in these instances where the VPA has a substantiated concern then consent does not have to be sought from the member.

Accuracy of Data and Keeping Data up to Date

The VPA has a responsibility to ensure members' information is kept up to date. Members will be required to let the Membership Secretary know if any of their personal information changes.

Accountability and Governance

The VPA Committee is responsible for ensuring that the VPA remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The VPA Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within the VPA and the reasons for this. Committee The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

 © Holmer Green VPA, 2026

Secure Processing

The Committee Members of the VPA have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee Members using strong passwords
- Committee Members not sharing passwords
- Restricting access of sharing member information to those on the Committee who need to communicate with members 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 Committee Members
- (If necessary), paying for firewall security to be put onto Committee Members' laptops or other devices.

Subject Access Request

VPA members are entitled to request access to the information that is held by the VPA. The request needs to be received in the form of a written request to the Membership Secretary of the VPA. 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 VPA 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.

Data Breach Notification

Were a data breach to occur, action shall be taken to minimise the harm by ensuring all Committee Members are aware that a breach had taken place and how the breach had occurred. The Committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. Where necessary, the Information Commissioner's Office would be notified. The committee shall also contact the relevant VPA members to inform them of the data breach and actions taken to resolve the breach.

If a VPA member contacts the VPA to say that they feel that there has been a breach by the VPA, a Committee Member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the Committee Member will ask the VPA member to follow this up with an email or a letter detailing their concern. The concern will then be investigated by Members of the Committee 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.

This Policy will bew reviewed and revised if and when there is a change in the UK's data protection regulations.

Signed on behalf of the VPA Committee:

Date: 1 February 2026

 © Holmer Green VPA, 2026