Burton Bradstock Village Society Data Protection Policy:

Privacy Policy

The Burton Bradstock Village Society (BBVS) collects only the following personal information:

Name, address, telephone number, email address.

Under "Legitimate Interests" when you join the Village Society this data will be used to provide you with information pertaining to the smooth running of the Society and its activities. Personal data will only be kept for as long as necessary to support Village Society activities.

The BBVS will not provide your personal information to any other party.

You can ask for your personal information to be deleted by contacting the Data Controller who is the Honorary Secretary of the Society

Note: This Privacy Policy will be available to any member wishing to view it on http//www.burtonbradstock.org.uk under the Village Society heading or by contacting the Honorary secretary.

Data Controller

The Honorary Secretary of the BBVS committee will take all appropriate steps as Data Controller to ensure that the BBVS conforms to the requirements of the Data Protection Act (2018). In particular

- That a public Privacy Policy is available as printed copies or PDF on request.
- That all forms that collect personal data include a Notice stating what is being collected and why.
- That all personal data is deleted when no longer needed.
- That all those who hold electronic files containing personal data are aware of their responsibilities, and take adequate precautions to hold that data securely.
- That any request or complaint is handled promptly and appropriately
- That any potential loss or compromise of personal data is handled in a proper and timely manner.

Paper records are included for completeness.

Should anyone contact a file owner asking that their personal details be removed, that request should be passed to all other owners of electronic files.

Any loss or compromise of personal data must be reported as soon as identified to the Data Controller by the file owner.

Those responsible for electronic files must ensure that adequate security is in place, including:

- reliable firewall and anti-virus systems that are maintained up-to-date.
- the operating system (e.g. Windows) and other key software (including security software and browsers) kept up-to-date with critical patches issued by the supplier.
- a reliable anti-spyware detection package is run at regular intervals to scan for malware.
- minimise the opportunity for compromise by, for example, using spam filters on emails, not opening suspect emails and not visiting suspect web sites.
- regularly back-up files/databases, and checks made that these back-ups are recoverable.