Data Protection Policy
Abergavenny Orchestral Society

Abergavenny Orchestral Society needs to gather and use certain information about individuals. This can include members, occasional players and other people who we may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the society's data protection standards and to comply with the law.

Why this policy exists

The data protection policy ensures that the society:

- complies with data protection law and follows good practice
- protects the rights of members and other contacts
- is open about how it stores and processes individuals' data
- takes appropriate measures to avoid a data breach

Data protection law

The data protection act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically or on paper. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The data protection act is underpinned by eight important principles. These say that personal data must:

- be processed fairly and lawfully
- be obtained only for specific lawful purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be held for any longer than necessary
- processed in accordance with the rights of data subjects
- be protected in appropriate ways
- not be transferred outside the European Economic Area, unless that country or territory also ensures an adequate level of protection

General guidelines

- The only people able to access the data covered by this policy should be those who need it to carry out tasks on behalf of Abergavenny Orchestral Society
- Data should not be shared informally
- Those with access to personal data should keep it secure by taking sensible precautions and following the guidelines below
- In particular, strong passwords should be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the society or externally

- Data should be kept up to date. If it is no longer required it should be deleted and disposed of.
- Ask for help if there is any aspect of data protection you are unsure of

Data access

Members of the committee are permitted to access personal data as needed to carry out tasks on behalf of the society. Access may also be granted by the committee to additional people for a specific purpose, e.g. first aiders may need access to medical details.

Data storage

These rules describe how and where personal data should be safely stored.

When data is stored on paper it should:

- be kept in a secure place where unauthorised people cannot see it
- not be left around where unauthorised people might see it
- be shredded and disposed of when no longer required

When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Online data should be stored only on secure cloud services and protected with strong passwords
- Data should not be stored on removable media (CD, memory stick)
- Data should not be downloaded to individuals' PCs or mobile devices

Data accuracy

In order to ensure that data is accurate and up to date we will take the following steps:

- Data will be kept in as few places as possible
- Duplication of data will be avoided as far as possible
- Inaccuracies are to be corrected as soon as possible
- Redundant or unnecessary data is to be removed

Subject access requests

All individuals who are the subject of personal data held by the society are entitled to:

- ask what information the society holds about them and why
- ask how to gain access to it
- be informed how to keep it up to date
- be informed how the society is meeting its data protection obligations

Requests for information can be made in person or by email. When responding to an email request, the identity of the person making the request must be verified before handing over any information.

Monitoring and review

The E-safety Officer is responsible for monitoring the effectiveness of this policy. This policy will be reviewed every two years.

Date of last review:

Date of next review:

Signed:……E-safety Officer

Signed:……Chairman