Data Protection policy

Introduction

In order to operate, The British Association of Barbershop Singers (BABS) needs to gather, store and use certain forms of information about individuals.

These can include members, employees, contractors, suppliers, volunteers, audiences and potential audiences, business contacts and other people the group has a relationship with or regularly needs to contact.

This policy explains how this data should be collected, stored and used in order to meet BABS data protection standards and comply with the General Data Protection Regulations (GDPR).

Why is this policy important?

This policy ensures that BABS:

- Protects the rights of our members, volunteers and supporters
- Complies with data protection law and follows good practice
- Protect the group from the risks of a data breach

Roles and Responsibilities

Who and what does this policy apply to?

This applies to *all* those handling data on behalf of BABS e.g.:

- Board members
- Volunteers
- Members
- Contractors/3rd-party suppliers

It applies to all data that BABS holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Any other personal information held (e.g. financial)

Roles and responsibilities

BABS is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for BABS is Alistair Lamyman. They, together with the Board of

Trustees, are responsible for the secure, fair and transparent collection and use of data by BABS. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

Everyone who has access to data as part of BABS has a responsibility to ensure that they adhere to this policy.

BABS uses third party Data Processors (e.g. White Fuse) to process data on its behalf. BABS will ensure all Data Processors are compliant with GDPR.

Data Protection Principles

a) We fairly and lawfully process personal data in a transparent way

BABS will only collect data where lawful and where it is necessary for the legitimate purposes of the group.

- A member's name, contact details and Gift Aid consent will be collected when they first join the group, and will be used to contact the member regarding group membership administration and activities. Other data may also subsequently be collected in relation to their membership, including their payment history for 'subs'. Where possible BABS will anonymise this data
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to BABS completing tasks expected as part of the individual's membership).

- The name and contact details of volunteers, employees and contractors will be collected when they take up a position, and will be used to contact them regarding group administration related to their role.

  Further information, including personal financial information and criminal records information may also be collected in specific circumstances where lawful and necessary (in order to process payment to the person or in order to carry out a DBS check).
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to BABS completing tasks expected as part of working with the individuals),

- An individual's name and contact details will be collected when they make a booking for an event. This will be used to contact them about their booking and to allow them entry to the event.
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to BABS completing tasks expected as part of the booking),

- An individual's name, contact details and other details may be collected at any time (including when booking tickets or at an event), with their consent, in order for BABS to communicate with them about and promote group activities. See 'How we get consent' below.
    - Lawful basis for processing this data: Consent (see 'How we get consent')

- Pseudonymous or anonymous data (including behavioural, technological and geographical/regional) on an individual may be collected via tracking 'cookies' when

they access our website or interact with our emails, in order for us to monitor and improve our effectiveness on these channels. See 'Cookies on the BABS website' below.
    - Lawful basis for processing this data: Consent (see 'How we get consent')

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, BABS will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

c) We ensure any data collected is relevant and not excessive

BABS will not collect or store more data than the minimum information required for its intended purpose.

d) We ensure data is accurate and up-to-date

BABS will ask members, volunteers and staff to check and update their data on an annual basis. Any individual will be able to update their data at any point by contacting the Data Protection Officer.

e) We ensure data is not kept longer than necessary

BABS will keep records for no longer than is necessary in order to meet the intended use for which it was gathered (unless there is a legal requirement to keep records).

The storage and intended use of data will be reviewed in line with BABS' data retention policy. When the intended use is no longer applicable (e.g. contact details for a member who has left the group), the data will be deleted within a reasonable period.

f) We keep personal data secure

BABS will ensure that data held by us is kept secure.

- Electronically-held data will be held within a password-protected and secure environment.
- Data is not to be stored on personal computing devices.
- Passwords for electronic data files will be reset each time an individual with data access leaves their role/position
- Physically-held data (e.g. membership forms or email sign-up sheets) will be stored in a locked cupboard
- Keys for locks securing physical data files should be collected by the Data Protection Officer from any individual with access if they leave their role/position. The codes on combination locks should be changed each time an individual with data access leaves their role/position
- Access to data will only be given to relevant trustees/committee members/contractors where it is clearly necessary for the running of the group. The Data Protection Officer will decide in what situations this is applicable and will keep a master list of who has access to data

g) Transfer to countries outside the EEA

BABS will not transfer data to countries outside the European Economic Area (EEA), unless the country has adequate protection for the individual's data privacy rights.

Individual Rights

When BABS collects, holds and uses an individual's personal data that individual has the following rights over that data. BABS will ensure its data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights.

Individual's rights

- *Right to be informed:* whenever BABS collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.

- *Right of access:* individuals can request to see the data BABS holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection Officer and will be complied with free of charge and within one month. Where requests are complex or numerous this may be extended to two months

- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. BABS will request that members, staff and contractors check and update their data on an annual basis. Any requests for data to be updated will be processed within one month.

- *Right to object:* individuals can object to their data being used for a particular purpose. BABS will always provide a way for an individual to withdraw consent in all marketing communications. When we receive a request to stop using data we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.

- *Right to erasure:* individuals can request for all data held on them to be deleted. BABS' Data Retention Policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made we will comply with the request unless:
    - There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.
    - There is a legal requirement to keep the data.
- *Right to restrict processing:* individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, BABS will restrict the data while it is verified).

Though unlikely to apply to the data processed by BABS, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Individual Contact

We only share members' data with other members with the subject's prior consent.

As a membership organisation BABS encourages communication between members.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Protection Office. These details will be given, as long as they are for the purposes of contacting the subject (e.g. an email address, not financial or health data) and the subject has consented to their data being shared with other members in this way

How we get Consent

BABS will regularly collect data from consenting supporters for marketing purposes. This includes contacting them to promote performances, updating them about group news, fundraising and other group activities.

Any time data is collected for this purpose, we will provide:

- A method for users to show their positive and active consent to receive these communications (e.g. a 'tick box')
- A clear and specific explanation of what the data will be used for (e.g. 'Tick this box if you would like BABS to send you email updates with details about our forthcoming events, fundraising activities and opportunities to get involved')

Data collected will only ever be used in the way described and consented to (e.g. we will not use email data in order to market 3rd-party products unless this has been explicitly consented to).

Every marketing communication will contain a method through which a recipient can withdraw their consent (e.g. an 'unsubscribe' link in an email). Opt-out requests such as this will be processed within 14 days.

Data Breaches

BABS takes any breach of data seriously. A data breach could be the deliberate or accidental:

- Loss of data – e.g. not knowing where physical or digital data is stored or how to access it, including devices being lost or stolen.
- Destruction of data – both physical and digital
- Corruption of data – e.g. changing data without permission or good reason or changing it with permission or good reason but incorrectly, either by BABS volunteers or third parties
- Unauthorised use of data e.g. sending an email that requires consent where consent has not been given.
- Unauthorised access to data – e.g. an (unauthorised) third party gains access to data stored by BABS
- Unauthorised disclosure of data – e.g. BABS passing data to a third party where we do not have a lawful basis to do so.

BABS acknowledges that a data breach can occur through both action and inaction on the part of the Data Controller or Processor.

How we prevent Data breaches

BABS has the following safeguards to ensure against possible data breaches:

- Data is stored on secure systems with access controlled by passwords
- Automatic, and manual, processes ensure passwords are updated on a regular basis, including as soon as an individual's role within, or relationship to, BABS changes.

- Automatic, and manual, processes ensure mass communications are only sent in line with mailing preferences.

If a Data breaches occurs

If anyone associated with BABS thinks a data breach has occurred then it should be reported to the Data Protection Officer immediately.

The Data Protection Officer will work with relevant individuals to investigate the potential breach. The response plan will include the following steps:

- Establish if a breach has occurred.
- Investigate if any measures can be taken to contain or minimise the breach.
- Establish the full extent and nature of that breach – including what the breach was, how many data subjects are affected and who they are.
- Establish if the data breach has, or is likely to, pose a significant risk to the data subjects rights and freedoms:
    - If the breach does pose a significant risk to the data subjects rights and freedoms we will:
        - Ensure all trustees are informed
        - Report the breach to the ICO. This will be done in-line with their guidelines and as soon as possible, but no later than 72 hours after the breach occurred
        - Report the breach to any other relevant regulators, including the Charity Commission.
        - Report the breach to the data subjects affected, informing them of what has happened, possible and likely impacts it might have on them and what we are doing to manage the breach and reduce risk of future occurrences
    - If the breach does not pose a significant risk to the data subjects rights and freedoms we will:
        - Document details of the breach and the decision making process involved in assessing the severity and risk of the breach.
        - Ensure the breach is reported to the Board of Trustees at the next planned full board meeting.

Conduct an internal investigation into how the breach happened and what measures need to be taken to minimise the risk of similar breaches occurring in the future.

Cookies on the BABS Website

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

BABS uses cookies on our website www.singbarbershop.com in order to monitor and record their activity. This allows us to improve users' experience of our website by, for example, allowing for a 'logged in' state, and by giving us useful insight into how users as a whole are engaging with the website.

We will implement a pop-up box on www.singbarbershop.com that will activate each new time a user visits the website. This will allow them to click to consent (or not) to continuing with cookies enabled, or to ignore the message and continue browsing (i.e. give their implied consent).

Policy Review

This policy will be reviewed every 2 years by the Board of Trustees. It will also be reviewed in response to changes in relevant legislation, good practice, or in response to an identified failing in its effectiveness. Members of the BABS Council will be informed of any changes to the policy and be invited to comment.



Alistair Lamyman
BABS Director of Administration



Shanna Wells
BABS Chair

Version Control - Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	July 2024	Initial draft approved	Annually
1.0.1	Board	July 2025	None	Annually