BRACKNELL CHORAL SOCIETY

DATA PROTECTION POLICY

1. Statement of intent

In order to operate, Bracknell Choral Society (BCS) needs to gather, store and use certain forms of information about individuals. These can include members, contractors, suppliers, volunteers, audiences and potential audiences, business contacts and other people the Society has a relationship with or regularly needs to contact.

This Policy explains how this data is collected, stored and used in order to meet BCS's data protection standards and comply with the UK General Data Protection Regulations (GDPR). A separate Data Retention Policy covers our data retention rules and together they form the BCS Privacy Policy.

This Policy ensures that BCS:

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

Please note that BCS does not use Cookies on its website.

2. Responsibilities

Overall responsibility for Data Protection rests with the Trustees / Committee of BCS, supported and advised by the Information Officer who acts as the Data Protection Officer (DPO).

Who and what does this policy apply to?

This Policy applies to all those handling data on behalf of BCS e.g.:

- Trustees / Committee members
- Volunteers
- Members, e.g. Part Stewards, Librarian and Event Organisers
- Contractors / 3rd-party suppliers e.g. Google, , TicketSource

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

- Names
- Email addresses
- Postal addresses
- Phone numbers and emergency contact
- Voice part
- Dietary information
- Accessibility needs
- Photograph
- Any other personal information held (e.g. financial)
- Roles and responsibilities
- Attendance
- Gift Aid

The Data Protection Officer (DPO), on behalf of the Committee, will determine what data is collected and how it is used. The DPO at BCS is the Information Officer (Pauline Williams). They, together with the Committee, are responsible for the secure, fair and transparent collection and use of data by BCS. In principle no data will be given to a user in excess of that needed for them to do the task they have to perform. Any questions relating to the collection or use of data should be directed to the DPO.

Everyone who has access to data as part of BCS has a responsibility to ensure that they adhere to this Policy. If and when BCS uses any 3rd-party Data Processors to process data on its behalf (e.g. Google, TicketSource, Making Music/Harmony), BCS will ensure all Data Processors are compliant with UK Data Protection law.

3. Data protection principles

Membership data

BCS will only collect data where lawful and where it is necessary for the legitimate purposes of the Society. A member's name and contact details will be collected when they first join the Society and will be used to contact the member regarding BCS membership administration and activities. Other data may also subsequently be collected in relation to their membership, such as payment history for subscriptions and Gift Aid for taxation purposes, dietary information ahead of away day participation, accessibility for concert participation .

Lawful basis for processing this data: Contract

Volunteers and contractors data

The name and contact details of volunteers and contractors (e.g. soloists and musicians) may be collected when they take up a particular role and will be used to contact them for matters related to their role. In some cases biographical information will also be retained.

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 to carry out a Disclosure and Barring Service (DBS).

Lawful basis for processing this data: Contract

Audience data

An individual's name and contact details may be collected when they make a booking for an event via TicketSource. This will be only used to contact them about their booking and to allow them entry to the event. If the event is cancelled, TicketSource automatically issue a refund to the individual.

Lawful basis for processing this data: Contract

An individual's name, contact details and other details may be collected at any time (including when booking tickets or at an event via TicketSource), with their consent, in order for BCS 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')

General principles

We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes. BCS will prompt members to check and update their data on an annual

basis, when requesting subscription payments. All fully paid BCS members will be given access to the secure Members' area of the website. They will be able to choose their own password and then input or amend their own personal information. In addition, if they have difficulties in doing this, any individual will be able to request an update to their data at any point by contacting the Data Protection Officer/Information Officer. Members can choose to upload a personal photograph or not.

BCS 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). See the Data Retention Policy for more details.

The storage and intended use of data will be reviewed by the Committee every 2 years in line with BCS's Data Retention Policy.

Keeping personal data secure

BCS will ensure that data held is kept secure. Electronically - held data will be held within a password-protected and secure environment. If a Committee member or Trustee leaves the Society, passwords for sensitive information e.g. member database, financial records will be updated.

Access to data will only be given to relevant Trustees / Committee members and Committee-appointed helpers where it is clearly necessary for the running of the group. The Data Protection Officer (DPO) will ensure that access to the shared Google Drive (where Trustee and Committee data is held) and the Making Music Platform for BCS (where the member database and its associated information is securely held), is protected with passwords and access delimited to the need to access the information. For example, the Treasurer would be permitted access to the financial information and member database, in order to invoice members for their subscriptions. However, they would not be allowed access to send the weekly newsletter.

Transfer to countries outside the UK

BCS will not transfer data to countries outside the UK unless the country has adequate protection for the individual's data privacy rights. Data held by 3rd-party suppliers or data controllers will conform to current UK Data Protection legislation.

Individual rights

When BCS collects, holds and uses an individual's personal data, that individual has the following rights over that data. BCS 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 BCS collects data it will explain why it is being collected and how it will be used.

Right of access: individuals can request to see the data BCS holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection Officer.

Right to rectification: individuals can update their own data or request that their data be updated where it is inaccurate or incomplete and must inform the Society of any change in contact details. 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. BCS will always

provide a way for an individual to withdraw consent in all marketing communications. Where 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. BCS's Data Retention Policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose for which 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, BCS will restrict the data while it is verified.

Member-to-member contact

This section applies to members who do not hold a position such as Part Steward or Librarian, with a legitimate need for contact details.

We only share members' data with other members with the subject's prior consent. The member secure area on the Bracknell Choral Society website (bracknellchoral.org.uk) shows other members their name, voice part and photograph only. The public cannot see this information. As a membership organisation BCS encourages communication between members. To facilitate this, members can request the personal contact data of other members in writing via the Secretary or Information Officer. These details will be given, as long as the need to contact the subject is reasonable and the subject has consented to their data being shared with other members in this way.

It is our policy that emails sent to the whole choir should always have members' email addresses placed in blind copy ('bcc').

How We Get Consent

BCS may collect data from consenting supporters for marketing purposes. This may include contacting them to promote performances, updating them about group news, fundraising and other group activities. Any time data is collected for these purposes, we will provide:

- A method for users to show their positive and active consent to have their data stored or to receive these communications (e.g. an Opt In 'tick box', response to an email request noted)
- A clear and specific explanation of what the data will be used for (e.g. 'Tick this box if you would like BCS 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).
- Any 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

BCS 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 BCS members, volunteers or 3rd-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) 3rd-party gains access to data stored by BCS
- Unauthorised disclosure of data – e.g. BCS passing data to a 3rd-party where we do not have a lawful basis to do so.

BCS acknowledges that a data breach can occur through both action and inaction on the part of the Data Controller or Processors (e.g. Chair, Secretary, Treasurer, Webmaster, Information Officer).

How we prevent Data breaches

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

- Data is stored on secure systems (either on the shared BCS Google Drive, the Making Music / Harmony secure BCS website or the personal computers of Committee members and their assistants) with password-protected access. The membership database has additional password protection to the secure website with limited access rights.
- BCS will ensure that access rights are updated on a regular basis, including as soon as an individual's role within, or relationship to, BCS changes.
- Automatic, and manual, processes ensure mass communications are only sent in line with mailing preferences.

If a Data breach occurs

If anyone associated with BCS thinks a data breach has occurred then it should be reported to the Data Protection Officer/Information Officer immediately. If not available, report it to the Chair and Secretary (Trustees).

The Data Protection Officer/Trustees 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 Committee meeting.

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

4. Review

This Policy will be reviewed every 2 years by the BCS Trustees / Committee.