# Blackburn Symphony Orchestra

## Data Protection policy

### July 2023 to August 2024

#### Introduction

In order to operate we need to gather, store and use data about our members, volunteers, friends, audience, business contacts and others with whom we have a relationship.

This policy explains how we will collect, store and use this data in order to comply with the UK General Data Protection Regulations (GDPR).

#### Roles and responsibilities

We are aware that we need to designate a Data Controlling Body (DCB hereafter) and a Data Protection Officer (DPO hereafter)

We have determined that our DCB shall be our existing Trustee Committee . The DCB, will determine what data is collected and how it is used. Our DPO will be our Honorary Secretary. They together with the trustee committee will be responsible for the secure, fair and transparent collection use of data. Any questions relating to the collection or use of data should be directed to the DPO.

Everyone who has access to our data has been made aware of their responsibility to:

- Protect the rights of the groups listed above
- Comply with data protection law and follow good practice
- Protect the group from the risks of a data breach.

This applies to our:

- Trustees
- Volunteers
- Members
- Friends
- Audience

It applies to all data that we hold relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Preferences regarding photography and Gift Aid

**We will only collect and use personal data for specific, explicit and legitimate purposes. We will only collect and store the minimum amount of data for these intended purposes**

- A member's name and contact details 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 we will anonymise this data.

- The name and contact details of volunteers 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 carry out a DBS check.

- An individual's name and contact details may 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.

We will ask members and volunteers 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.

We will not keep records for any 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 our data retention policy. When the intended use is no longer applicable the data will be deleted as soon as possible.

**To ensure security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage we will adopt the following procedures**

- Electronically-held data will be held within a password-protected and secure environment
- Passwords for electronic data files will be re-set each time an individual with data access leaves their role/position
- BSO do not have offices. Where Trustees require access to physical data they will store it in locked when unattended locations.
- Physical data files should be collected by the Data Protection Officer from any individual if they leave 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.

- No individual will have permission to transfer data, by any means, outside the orchestra's password protected Google account.

# An individual's rights

We recognise that individuals have rights over the data we hold on them. We will ensure data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights as listed below

- *Right to be informed:* whenever we collect data we 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 we hold 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 a week. Where requests are complex or numerous this may be extended to two weeks.
- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. We will request that members, check and update their data on an annual basis. Any requests for data to be updated will be processed within one week.
- *Right to object:* individuals can object to their data being used for a particular purpose. We 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. Our 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

As a membership organisation we encourage communication between members .To facilitate this:

- Members may request the contact data of other members in writing via the Data Protection Officer. These details will be given as long as they are for the purposes of contacting the subject and the subject has consented to their data being shared with other members in this way.

**Marketing Purposes**

We may from time too time 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 BSO 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. 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

We take the threat of breach of data seriously whether deliberate or accidental. We acknowledge that a data breach can occur through both action and inaction on our part.

- 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, by anyone.
- 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 our data.
- Unauthorised disclosure of data by us passing data to a third party where we do not have a lawful basis to do so.

## How we intend to prevent 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, BSO changes.
- Automatic, and manual, processes ensure mass communications are only sent in line with mailing preferences.

## If a Data breach occurs

A suspected data breach should be reported to the DPO/trustees immediately.
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 planed 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.

# Data retention policy

## Introduction

This policy sets out how we will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of our Data Protection Policy.

## Roles and responsibilities

The Trustee Committee is the Data Controller Body and will determine what data is collected, retained and how it is used. Our Data Protection Officer together with the Trustee Committee are responsible for the secure and fair retention and use of BSO data. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

A regular review of all data will take place to establish if we still have good reason to keep and use data held at the time of the review.

As a general rule a data review will be held every year and no more than 24 calendar months after the last review. The next review will take place on 1st August 2024

## Data to be reviewed

- Data stored on third party online services
- Physical data stored at the homes of committee members

## Who the review will be conducted by

The review will be conducted by the Data Protection Officer with other committee members to be decided on at the time of the review.

## How data will be deleted

- Physical data will be destroyed safely and securely.
- All reasonable and practical efforts will be made to remove data stored digitally.
    - Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.
    - Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

## Criteria

The following criteria will be used to make a decision about what data to keep and what to delete.

| Question | Action | |
|---|---|---|
| | **Yes** | **No** |
| Is the data stored securely? | No action necessary | Update storage protocol in line with Data Protection policy |
| Does the original reason for having the data still apply? | Continue to use | Delete or remove data |

| | | |
|---|---|---|
| Is the data being used for its original intention? | Continue to use | Either delete/remove or record lawful basis for use and get consent if necessary |
| Is there a statutory requirement to keep the data? | Keep the data at least until the statutory minimum no longer applies | Delete or remove the data unless we have reason to keep the data under other criteria. |
| Is the data accurate? | Continue to use | Ask the subject to confirm/ update details |
| Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual | Continue to use | Get consent |
| Can the data be anonymised | Anonymise data | Continue to use |

## Statutory Requirements

Data stored by us may be retained based in statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declarations records
- Details of payments made and received (e.g. in bank statements and accounting records)
- Trustee meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax records

## Member data

- When a member leaves, and all administrative tasks relating to their membership have been completed, any potentially sensitive data held on them will be deleted Unless consent has been given data will be removed from all email mailing lists.
- All other data will be stored safely and securely and reviewed as part of the next two year review

## Mailing list data

- If an individual opts out of a mailing list their data will be removed as soon as is practically possible.
- All other data will be stored safely and securely and reviewed as part of the next annual review

## Volunteer data

- When a volunteer stops working with us and all administrative tasks relating to their work have been completed any potentially sensitive data held on them will be deleted – this might include bank details or medical data
- Unless consent has been given data will be removed from all email mailing lists
- All other data will be stored safely and securely and reviewed as part of the next annual review Other data
- All other data will be included in a regular annual review.