



## **Data Protection Policy**

**Note: The legal entity known as The Nottingham Harmonic Society is referred to throughout this document as Nottingham Harmonic Choir (or the Choir). The Officers and all the other General Committee Members are, and may be referred to as, the Trustees.**

### **1. Introduction**

To operate, the Nottingham Harmonic Choir needs to gather, store and use certain forms of information about individuals. These can include members, professionals, volunteers, contractors, suppliers, 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 to meet the Choir's data protection standards and comply with the law.

### **2. Why is this policy important?**

This policy ensures that the Choir:

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

### **3. Roles and responsibilities**

This policy applies to all those handling data on behalf of the Choir, e.g.:

- Committee members
- Professionals and volunteers
- Members
- Contractors/3<sup>rd</sup> party suppliers (where possible)

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

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

Everyone who has access to data as part of the Choir has a responsibility to ensure that they adhere to this policy. The Data Controller for the Choir is a nominated Trustee of the Society. This individual, together with the General Committee, is responsible for why data is collected and how it will be used. Any questions relating to the collection or use of data should be directed to the Data Controller.

## **4. Data Protection Principles**

### **a) Fair and lawful processing of personal data**

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

- i. A member's name and contact details will be collected when they first join the Choir and will be used to contact the member regarding choir membership administration and activities. Other data may also subsequently be collected in relation to their membership, including their payment history for choir subscriptions and other related costs.
- ii. The name and contact details of committee members, professionals and 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 (to process payment to the person or to carry out a DBS check).
- iii. 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.
- iv. An individual's name, contact details and other information may be collected at any time (including when booking tickets or at an event), with their consent, for the Choir to communicate with them about group activities, and/or for Direct Marketing. See 'Direct Marketing' below.

When collecting data, the Choir will always explain to the subject why the data is required and what it will be used for, e.g.

*"Please enter your email address in the form below. We need this so that we can send you email updates for group administration including about rehearsal and concert schedules, subs payments and other business."*

We will never use data for any purpose other than that stated or that can be considered reasonably to be related to it. For example, we will never pass on personal data to 3<sup>rd</sup> parties without the explicit consent of the subject.

### **b) We ensure any data collected is relevant and not excessive.**

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

As an illustration, we need to collect telephone numbers from members to be able to contact them about group administration, but data on their marital status, for example, will not be collected, since it is unnecessary and excessive for the purposes of group administration.

### **c) We ensure data is accurate and up to date**

The Choir will ask members, professionals 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 Controller.

#### **d) We ensure data is not kept longer than necessary**

The Choir will keep data on individuals for no longer than 12 months to meet the intended use for which it was gathered and after our involvement with the individual has stopped unless there is a legal requirement to keep records.

#### **e) We process data in accordance with individuals' rights**

The following requests can be made in writing to the Data Controller:

- Members, volunteers and supporters can request to see any data stored on about them. Any such request will be actioned within 14 days of the request being made.
- Members, volunteers and supporters can request that any inaccurate data held on them is updated. Any such request will be actioned within 14 days of the request being made.
- Members, volunteers and supporters can request to stop receiving any marketing communications. Any such request will be actioned within 14 days of the request being made.
- Members and supporters can object to any storage or use of their data that might cause them substantial distress or damage or any automated decisions made based on their data. Any such objection will be considered by the Data Controller or the General Committee, and a decision communicated within 30 days of the request being made.

#### **f) We keep personal data secure**

The Choir will ensure that data held by us is kept secure.

- 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.
- Physically held data (e.g., membership forms or email sign-up sheets) will be stored in a secure manner.
- Access to data will only be given to relevant trustees and contractors where it is clearly necessary for the running of the group. The Data Controller will decide in what situations this is applicable and will keep a master list of who has access to data.

### **5. Member to member contact**

We only share members' data with other members with that member's prior consent.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Controller or Membership Secretary. These details will be given, if they are for the purposes of contacting the member (e.g., an email address, not financial or health data) and the member consents to their data being shared with other members in this way.

The Choir will regularly collect data from consenting supporters for marketing purposes. This includes contacting them to promote concerts, updating them about group news, fundraising and other group activities. Whenever data is collected for this purpose, we will provide:

- A clear and specific explanation of what the data will be used for (e.g., *'Tick this box if you would like the Choir to send you email updates with details about our forthcoming events, fundraising activities and opportunities to get involved'*)

- A method for users to show their active consent to receive these communications (e.g., a 'tick box')
- Instructions and contact details for requesting the secure deletion of personal information held by the Choir, with a note explaining how this may impact on their membership of the Choir.

Data collected will only ever be used in the way described and consented to (e.g., we will not use email data to market third 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.

## **6. Cookies on the Choir 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.

The Choir uses cookies on our website [www.nottinghamharmonic.org](http://www.nottinghamharmonic.org) to provide essential website functionality. For members of the public, the primary role for these cookies is to permit the basic operation of the WordPress software which handles the presentation of site webpages. For choir members and site administrators, cookies are used to enable password-based secure access to the site control panels and member only pages.

Cookies are used to keep track of user preferences – for example whether a newsletter signup box has been presented to the website visitor in the previous 100 days.

The Choir employs a pop-up box on [www.nottinghamharmonic.org](http://www.nottinghamharmonic.org) that activates for each new visitor to the website (on first visit and subsequently at a minimum of once every 100 days). This will allow them to click to consent to continuing with cookies enabled, or to opt to allow essential cookies only.

The cookie consent system includes a link to a detailed summary of cookies used on the website and their function.

## **7. Data Breaches**

The Choir takes any breach of data seriously. A data breach could be deliberate or accidental. The Choir 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 in relationship to, the Choir changes.
- Automatic and manual processes ensure mass communications are only sent in line with mailing preferences.

If anyone associated with the Choir thinks a data breach has occurred, then it should be reported to the Data Controller/Trustees immediately. The Data Controller and Trustees will work with the relevant individuals to investigate the potential breach.

## 8. Data Retention

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

### a) Roles and responsibilities

The Data Controller will determine what data is collected, retained and how it is used. The Data Controller, together with the Trustees is responsible for the secure and fair retention and use of data by the Choir. Any questions relating to data retention or use of data should be directed to the Data Controller.

### b) Regular Data review

The data held by the Choir will be reviewed by the Data Controller every two years. The following criteria will be used to decide 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

The results of the data review will be shared with the members of the Choir's General Committee.

### c) Statutory Requirements

Data stored by the Choir may be retained based on 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.
- Insurance details.
- Tax and employment records.

## **d) Other Data Retention procedures**

### **Member data**

- When a member leaves the Choir 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 two-year review.

### **Volunteer and professional's data**

- When a professional or volunteer stops working with the Choir and all administrative tasks relating to their work have been completed any potentially sensitive data held on them will be deleted – such as 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 a next two-year review.

### **Other data**

- All other data will be included within the formal review taking place every two years.