

Cherwell Choral Society

Data Protection Policy



Overview

Key details:

- Policy first approved by committee and published: May 2018
- Updated: August 2021
- Next review date: October 2021 (after Society's AGM)

Introduction:

In order to operate, Cherwell Choral Society (CCS) 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 CCS's data protection standards and comply with the General Data Protection Regulations (GDPR).

Why is this policy important?

This policy ensures that CCS:

- 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

Roles and Responsibilities

This Policy applies to all those handling data on behalf of CCS, eg:

- Committee members
- Employees and volunteers
- Members
- Contractors/third-party suppliers

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

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

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

The **Data Controller** for CCS is the Chairman, Gill Nunn, and she will determine what data is collected and how it is used.

The **Data Protection Officer** is the Membership Secretary, Bobbie Koen.

They, together with the committee, are responsible for the secure, fair and transparent collection and use of data. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

If CCS uses any third party data processors (eg for ticket sales) to process data on its behalf they will ensure all Data Processors are compliant with GDPR.

Data Protection Principles

1. We fairly and lawfully process personal data in a transparent way

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

- 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'.
- The name and contact details of volunteers, committee members, 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).
- 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.
- 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 CCS to communicate with them about and promote group activities.

2. We only collect and use personal data for specified and lawful purposes.

When collecting data, CCS will always explain to the subject why the data is required and what it will be used for. For example: *Please enter your email address in the form below. We need this so that we can send you email updates including rehearsal and concert schedules, subs payments and other business.*

We will never use this 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 third parties without the explicit consent of the subject.

3. We ensure any data collected is relevant and not excessive

CCS will not collect or store more data than the minimum information required for its intended purpose. For example we need to collect telephone numbers from members in order to be able to contact them about group administration such as return of library music, but data on their marital status or sexuality will not be collected, since it is unnecessary and excessive for the purposes of group administration.

4. We ensure data is accurate and up-to-date

CCS 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 (Membership Secretary).

5. We ensure data is not kept longer than necessary

CCS 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 CCS's 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.

6. We keep personal data secure

CCS 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 locked cupboard
- Keys for locks securing physical data files should be collected by the Data Controller 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

7. Transfer to countries outside the EEA

CCS 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.

8. Taking and using photo and video images

- CCS will occasionally use photos/video footage for promoting the group. The rights, interests and freedoms of any individuals in the photos/videos will be considered.
- Members will be advised when photos/videos are being taken
- CCS will minimise the risk of someone being identified when their image is used publicly (for example captions will not be used)
- Permission will be sought for the use of close-ups
- All images will be stored anonymously

Individual Rights

When CCS collects, holds and uses a member's personal data, that individual has the following rights over that data. CCS 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 CCS collects data the individual will be advised to refer to this Policy to see why it is being collected and how it will be used.
- *Right of access:* individuals can request to see the data CCS 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. CCS 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. CCS 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. CCS's 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 legal requirement to keep the data.

Member-to-Member Contact

As a membership organisation CCS encourages communication between members.

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

Direct Marketing

CCS 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 CCS 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 and will be used to market third-party products only if the Data Protection Officer considers them to be of interest to members (eg events organised by other local choirs or organisations)

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 Retention Policy

Data Review

A regular review of all data will take place to establish if CCS still has good reason to keep and use the data held at the time of the review. As a general rule a data review will be held every two years.

The review will be conducted by the Data Protection Officer with other committee members to be decided on at the time of the review. The most recent review took place in **August 2021**.

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

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

Other Data Retention Procedures

Member data

- When a member leaves CCS and all administrative tasks relating to their membership 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 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

Employee data

- When an employee stops working with CCS 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 two year review

Other data

- All other data will be included in a regular two year review.