Data Protection Policy

Introduction

1. Winchester Community Choir ("WCC") keeps and processes a small amount of personal information about: it's current and former members; those who have enquired about membership of WCC and are waiting to join; and those who assist and support us as friends of the choir

2. WCC will keep the following categories of personal information:

Category	Examples	Purpose
Contact details	Email address, home and mobile telephone numbers and (in some cases postal address)	To communicate effectively with members and friends about the activities of the choir
Review dates and flags	The date a sabbatical (where a member takes a break from active participation in the choir) is to be reviewed; a flag to show that a member has volunteered to attend an optional activity	To administer membership of the choir and its activities
Financial information	Limited to records of subscription payments received and qualification for concessionary rates of subscription	To ensure that member subscriptions are up-to-date and appropriate
Other personal information	Gender and range of voice (e.g. Tune, Alto, Bass, Tenor)	To inform an assessment whether the balance of voices in the choir is appropriate
Attendance records	Records of attendance at choir sessions and apologies for absence	To follow up unexplained absences from choir sessions.
Offices held	Whether the member holds office on the Committee or performs any other special role in the Choir (e.g. Section Leader)	To ensure the effective running of the choir and its business
Correspondence	Email and other written communications with members	To keep a record of communications between members, the Committee and its officers

3. The managing committee of WCC (the "Committee") and its officers will ensure that this personal information: is collected and used lawfully[1]; is stored in a secure manner; is not stored longer than is strictly necessary; and is not used for any purpose other than the purpose for which it was provided (namely to organise the activities of the choir).

4. The lawful basis for keeping and processing this personal data is the explicit or implied consent of the individual.

5. The Committee is obliged to designate a person who is responsible for the protection of personal data. The Committee has designated the Membership Secretary for this role. The Membership Secretary can be contacted at: membership@winchestercommunitychoir.co.uk

6. The Membership Secretary will be responsible for: advising (or arranging for another to advise) the Committee and choir membership about their obligations to comply with legislation about data protection; monitoring compliance with data protection legislation. The Membership Secretary is the first point of contact in relation to data protection matters, including complaints

7. Any person (choir member or friend of WCC) who considers that this policy has not been followed in respect of personal data about him or herself should raise the matter with the Membership Secretary.

[1] The principal legislation in this area is the General Data Protection Regulation (EU) 2016/679 (GDPR). The GDPR aims primarily to give control to individuals over their personal data.

8. The Committee will respect the legal rights of its members and friends, which include: the right to be informed about the personal data held about them; the right of access to that data; the right to rectify errors in the data and the right to its erasure (with certain qualifications); the right to restrict processing[2]; the right to data portability[3]; the right to object to the processing of their personal data[4].

9. The Committee and its officers will not use personal data for automated decision making or for profiling its members and friends.

10. The Committee and its Officers will not transfer this data to a third party without the express consent of individual members.

11. Normally, the Committee will retain written and digital records about its members for six years after they leave the choir unless there are reasons permitted in law to keep the records for a longer period[5].

12. The Committee and its officers will implement technical and organisational measures to ensure that data is stored and processed securely.

13. The Committee will commission an investigation of any breach of data security or of its data protection arrangements and will consider whether such breach should be reported to the Information Commissioner's Office[6].

Current Technical and organisational measures

1. The main member database is maintained by the Membership Secretary in a Microsoft Excel workbook on a pin-protected PC with proprietary internet security installed. The data is backed up continuously to secure cloud storage with 256-bit AES encryption.
2. Extracts of the member database are uploaded weekly to DropBox for shared use by Committee members.
3. Non-member personal data, consisting of email lists, is maintained by the Website Editor and resides in an online database that is backed up to the cloud weekly with the rest of our website.

Version control

		Published
This version	1.0	21-Jan-2019
Previous versions	No previous versions	

Changes in this version

1	
2	
3	
4	

[2] **The right to restrict processing** means that an individual can limit the way that an organisation uses their data. This may be because they have issues with the content of the information or how it is processed.
[3] **The right to data portability** allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another.
[4] **The right to object** only applies in certain circumstances. For example, individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.
[5] Some leaver records do not have leaving dates. These records will be kept for six years from the date this policy is approved.
[6] WCC is a not-for-profit organisation and is exempt from having to register and pay a fee to the Information Commissioner's Office (ICO). Nonetheless, the ICO advises that any organisation that experiences a personal data breach needs to consider whether this poses a risk to people. It says, "You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO."