

Radlett Music Club
Data Protection and Retention Policy

1. Definitions

“**Club**” - means Radlett Music Club

“**Committee**” - means the Committee of the Club

“**GDPR**” - means the General Data Protection Regulations

“**Member**” - means an existing and/or established member of the Club and a prospective member providing personal data to the Club in anticipation of becoming a Member

“**Third Parties**” – means artists, volunteers, suppliers, contractors and others who are not Members but with whom the Club has dealings in the conduct of its activities

“**Website**” – means the Club’s website at <http://www.radlett-music-club.co.uk/>

2. Introduction

2.1. In order to operate, the Club needs to gather, store and use certain forms of information about Members and Third Parties.

2.2. This policy explains how this data will be collected, stored and used in order to meet the Club’s data protection standards and comply with the GDPR.

2.3. This policy was first approved and adopted by the Committee on 22 November 2018 and may be revised from time to time.

3. Roles and responsibilities

3.1. This policy applies to all those handling data on behalf of the Club. As regards electronic data stored with third party online services, such service providers will obviously not be bound by this policy but the Club will only use reputable service providers (e.g. Google Drive, iCloud, OneDrive, Amazon Glacier) who, it is presumed, will themselves have systems in place to provide security and comply with GDPR.

3.2. It applies to all data that the Club holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Subscription payment records
- Gift Aid declarations

3.3. The Club is the Data Controller for the purposes of GDPR and operates through its Committee. The Committee will determine what data is collected and how it is used, but always in accordance with this policy. Any questions relating to the collection or use of data should be directed in the first instance to either the Hon. Secretary or the Membership Secretary.

3.4. Everyone who has access to data as part of the Club has a responsibility to ensure that he or she adheres to this policy.

4. Principles relating to data collection, use, retention and protection

4.1. Data collection

- 4.1.1. The Club will only collect data where lawful and where it is necessary for the legitimate purposes of the Club. In particular:
 - 4.1.1.1. A Member's name and contact details will be collected when he or she first joins or applies to join the Club. Those details will be used to contact the Member regarding Club membership administration and activities. Subsequently, other data may also be collected in relation to such membership, including payment history for subscriptions and where contact details change.
 - 4.1.1.2. The names and contact details of Third Parties will be collected when they are necessary for the Club's activities and will be used to contact such persons regarding Club administration related to their role.
 - 4.1.1.3. When non-members make a booking for a Club concert, any relevant personal data (e.g. contact details) are collected by the Radlett Centre which is independent of the Club. The Club will not be passed such data and will have no control of it.
- 4.1.2. When collecting data from Members, the Club will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for. If the Club wants to use any data of a Member for any other purpose, the Club would first seek consent from such Member. The Club's privacy statement for Members is posted on the Website.
- 4.1.3. Under GDPR, the lawful basis for collecting, and using, such data is in contract i.e. it is implicit in being a Member that the Club does these things to enable the Member to benefit from the Club's primary activities. The same principle applies to the others referred to in paragraphs 4.1.1.2 above. It could also be said that the Club has a legitimate interest in collecting and using such data for such purposes. Under GDPR, it is not necessary to obtain consent for collecting and using data that is covered by 'contract' and/or 'legitimate interest'.

4.2. Data use

- 4.2.1. The Club will only use data for explicit and legitimate purposes, as disclosed in the privacy statement for Members. As regards Third Parties, the Club will only use data for the legitimate purposes relating to the Club's dealings with such Third Parties.
- 4.2.2. The only people able to access data covered by this policy should be those who need to communicate with the Members or with Third Parties in relation to the Club's activities, or who otherwise need such access in order properly to perform their Committee function.
- 4.2.3. The Club only shares Members' data with other Members with the subject's prior consent.
- 4.2.4. Data collected will only ever be used in the way described and consented to (e.g. the Club will not use email data in order to market 3rd-party events or products unless this has been explicitly consented to).

4.2.5. The provisions of this paragraph 4.2.5 are only applicable to Committee members. The Charity Commission has a statutory power to request the supply of certain personal data of charity trustees, which for the Club means Committee members, to enable the Charity Commission (1) to check that trustees are eligible to be trustees and (2) to contact trustees in certain circumstances. As at the date of this version of this policy, such data includes names, addresses, dates of birth, telephone numbers and email addresses. Any trustee who refuses to supply the information requested may be required by the Charity Commission to justify such refusal. Accordingly:

4.2.5.1. No such data shall be supplied to the Charity Commission without first seeking the individual consents of the Committee members.

4.2.5.2. Any Committee member who refuses to supply such data must be willing to justify such refusal to the Charity Commission and to accept the consequences of not doing so.

4.3. Data retention

4.3.1. A regular review of all data will take place to establish if the Club still has a valid reason to keep and use the data held at the time of the review.

4.3.2. As a general rule, a data review will be held every 2 years. The first review will take place during the few months following adoption of this policy.

4.3.3. Data to be reviewed:

- Data in digital form (e.g. spreadsheets) on personal devices (e.g. a computer or laptop) held by Committee members.
- Data stored on third party online services (e.g. Google Drive, iCloud).
- Physical data stored at the homes of Committee members.

4.3.4. The review will be conducted by the Membership Secretary, together with such other Committee members as may be decided on at the time of the review.

4.3.5. The criteria in Annex 1 will be used to make a decision about what data to keep and what to delete. If data is to be deleted:

- Physical data will be destroyed safely and securely, including shredding.
- All reasonable and practical efforts will be made to remove data stored digitally.

4.3.6. Data stored by the Club may be retained in the following circumstances:

4.3.6.1. Where deleting data would mean deleting other data that the Club has a valid and lawful reason to keep (e.g. in old emails) then the data may be retained securely but not used.

4.3.6.2. If there is a statutory requirement for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declaration records
- 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

4.3.7. The Club will ask Members 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 Club.

4.4. Data security

The Club will take reasonable steps to ensure that data held is kept secure. In particular:

4.4.1. Electronically-held data will be stored on personal devices belonging to the Membership Secretary and some other Committee members but such data is not generally held by every Committee member. Those Committee members who do hold such data will comply with the following:

4.4.1.1. log-on to his or her personal device will be protected by a reasonably strong password;

4.4.1.2. if access to a storage device (e.g. external hard drive, USB stick) is not protected by password or other encryption, then such devices shall only be used for data covered by this policy if the files containing such data are themselves protected by a suitable password or other form of encryption;

4.4.1.3. to the extent that such data is stored or backed-up with third party online services (see paragraph above 3.1):

- access to such services will be reasonably secure (e.g. by means of a reasonably strong password); and
- only reputable providers will be used.

4.4.1.4. Where members of the Committee need to share electronic data, and whether that data is transferred by email, USB stick or other means:

- access to the device used for the transfer (e.g. USB stick) must itself be password protected or the file being transferred must be password protected;
- if the file is sent by email, the file being transferred must be password protected; and
- the password access for the device or files containing such data may be shared between the Committee members concerned but the device or email containing the encrypted file should not itself contain the password which should be communicated by separate means (e.g. orally in person or on the telephone, or by text message but not by email).

4.4.1.5. Subject to paragraph 4.4.1.4, such log-on and access passwords will not be shared with other Committee members, nor anyone else.

4.4.2. In relation to physically-held data:

4.4.2.1. some documents (e.g. membership forms, contact details for those Members who do not use electronic devices etc.) will be stored by the Membership Secretary.

4.4.2.2. other types of documents (e.g. Gift Aid declarations) will be stored by other Committee members.

In each case, such documents will be kept in the homes of such Committee members which environment should be regarded as reasonably secure.

- 4.4.3. Access to data will only be given to relevant Committee members or Third Parties where it is clearly necessary for the running of the Club.

5. Individual's rights

5.1. When the Club collects, holds and uses an individual's data, that individual has the following rights over that data.

- 5.1.1. *Right to be informed:* by the provision of a clear and specific privacy statement explaining why it is being collected and how it will be used.
- 5.1.2. *Right of access:* to see the data that the Club holds on such person.
- 5.1.3. *Right to rectification:* to require that data be corrected where it is inaccurate or incomplete.
- 5.1.4. *Right to object:* to the data being used for a particular purpose. The Club will comply with such a request unless the Club has a lawful reason to hold or use the data for legitimate interests or contractual obligation.
- 5.1.5. *Right to erasure:* for all data held on such person to be deleted. The Club will comply with the request (subject to the issue concerning back-up systems referred to in paragraph 5.2 below), unless the Club has a lawful reason to keep it (see paragraph 4.3.6 above).

5.2. As regards deletion of data from back-up systems:

- 5.2.1. the Club will delete data as required by this policy from systems in the direct control of the Club;
- 5.2.2. where the data is backed-up with third party online services (see paragraph 4.4.1.3 above) whose own back-up systems are self-evidently outside the control of the Club, the Club will take reasonable steps to secure deletion of such data or, failing that, to 'put beyond use' such data within the meaning of that phrase as given in guidance issued by the Information Commissioner's Office.

5.3. The Club will make all reasonable efforts to fulfil requests from an individual in relation to such rights.

6. Cookies on the Website

- 6.1. 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.
- 6.2. The Club uses cookies on the Website in order to monitor and record a user's activity. This allows the Club to improve a user's experience of the Website.
- 6.3. The Club will implement a pop-up box on the Website that will activate each time a new user visits the Website. This will allow such user to ignore the message and continue browsing (i.e. give their implied consent). Alternatively, the user can click to opt out of the use of the Website cookies but, in doing so, it should be noted that a limited number of cookies will still be used to run the Website and some aspects of the Website may not work as well without tracking cookies.
- 6.4. The Website will also include a link to this policy which specifies that cookies are used.

Annex 1

Data Protection and Retention Policy

Question	Action	
	Yes	No
Is the data stored securely?	No action necessary	Update storage protocol in line with this Data Protection policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data, save where the data is backed-up with third party online services where the provisions of paragraph 5.2 of this Data Protection Policy shall apply)
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 lawful reason to keep the data? (See paragraph 4.3.6 of this Data Protection policy)	Keep the data. If there is a statutory requirement, at least keep it until the statutory minimum period 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