DATA PROTECTION

AND RETENTION POLICY

PART 1: DATA PROTECTION

1. Introduction

In order to operate, Dorset Sinfonia needs to gather, store and use certain forms of information about individuals.

These can include members, employees, 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 Dorset Sinfonia's data protection standards and comply with the General Data Protection Regulations (GDPR).

This policy ensures that Dorset Sinfonia:

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

2. Roles and responsibilities

This applies to *all* those handling data on behalf of Dorset Sinfonia e.g.:

- Trustees
- Employees
- Members

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

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

Dorset Sinfonia is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for Dorset Sinfonia is Jo Rowe. They,

together with the other Trustees, are responsible for the secure, fair and transparent collection and use of data by Dorset Sinfonia. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

Everyone who has access to data as part of Dorset Sinfonia has a responsibility to ensure that they adhere to this policy.

3. Data protection principles

a) We fairly and lawfully process personal data in a transparent way

Dorset Sinfonia 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' and any gift aid declaration.
  Where possible Dorset Sinfonia will anonymise this data
  - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to Dorset Sinfonia completing tasks expected as part of the individual's membership).

- The name and contact details of employees 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).
  - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to Dorset Sinfonia completing tasks expected as part of working with the individuals),

- 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 Dorset Sinfonia to communicate with them about and promote group activities. See 'How we get consent' below.
  - Lawful basis for processing this data: Consent (see 'How we get consent')

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, Dorset Sinfonia 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.

c) We ensure any data collected is relevant and not excessive

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

E.g. we need to collect email addresses from members in order to be able to contact them about group administration, but data on their marital status or sexuality will not be collected, since it is unnecessary and excessive for the purposes of group administration.

d) We ensure data is accurate and up-to-date

Dorset Sinfonia 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.

e) We ensure data is not kept longer than necessary

Dorset Sinfonia 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 Part 2 of this 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.

f) We keep personal data secure

Dorset Sinfonia 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, email sign-up sheets or gift aid declarations) will be stored in a locked cupboard
- Keys for locks securing physical data files should be collected by the Data Protection Officer from any individual with access if they leave their role/position.
- Access to data will only be given to relevant committee members 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.

4. Individual rights

When Dorset Sinfonia collects, holds and uses an individual's personal data that individual has the following the rights over that data. Dorset Sinfonia 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.

An individual's rights are as follows:

- *Right to be informed:* whenever Dorset Sinfonia collects data it 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 Dorset Sinfonia 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. Dorset Sinfonia 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. Dorset Sinfonia 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. Dorset Sinfonia'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 lawful reason to keep and use the data for legitimate interests or contractual obligation.
  - There is a legal requirement to keep the data.

- *Right to restrict processing:* individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if

they have contested the accuracy of any of their data, Dorset Sinfonia will restrict the data while it is verified).

Though unlikely to apply to the data processed by Dorset Sinfonia, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

5. Member-to-member contact

We only share members' data with other members with the subject's prior consent.

As a membership organisation Dorset Sinfonia encourages communication between members.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Protection Officer or 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

6. How we get consent

Dorset Sinfonia may 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 Dorset Sinfonia 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 (e.g. we will not use email data in order to market 3rd-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.

7. Data breaches

Dorset Sinfonia takes any breach of data seriously. A data breach could be the deliberate or accidental:

- 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, either by Dorset Sinfonia staff, volunteers or third parties
- 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 data stored by Dorset Sinfonia
- Unauthorised disclosure of data – e.g. Dorset Sinfonia passing data to a third party where we do not have a lawful basis to do so.

Dorset Sinfonia acknowledges that a data breach can occur through both action and inaction on the part of the Data Controller or Processor.

How we prevent Data breaches

Dorset Sinfonia 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 relationship to, Dorset Sinfonia changes.
- Manual processes ensure mass communications are only sent in line with mailing preferences.

If a Data breach occurs

If anyone associated with Dorset Sinfonia thinks a data breach has occurred then it should be reported to the Data Protection officer immediately.

The Data protection officer 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.

PART 2: DATA RETENTION

8. Introduction

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

It forms part of Dorset Sinfonia's Data Protection Policy.

9. Roles and responsibilities

Dorset Sinfonia is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for Dorset Sinfonia is Jo Rowe. They, together with the committee are responsible for the secure and fair retention and use of data by Dorset Sinfonia. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

10. Regular data review

A regular review of all data will take place to establish if Dorset Sinfonia 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 2 years and no more than 27 calendar months after the last review. The latest review took place in Sept 2021.

Data be reviewed:

- Dorset Sinfonia stores data on digital documents (e.g. spreadsheets) stored on personal devices held by committee members.
- Physical data stored at the homes of committee members.

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, including shredding.
- 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.

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

Date stored by Dorset Sinfonia 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)
- Committee meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax and employment records

11. Other data retention procedures

Member data

- When a member leaves Dorset Sinfonia 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 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.

Volunteer and freelancer data

- When a freelancer stops working with Dorset Sinfonia 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.

Written: May 2018

Reviewed every 2 years. Last reviewed: Sept 2026