



Kala Data Privacy Policy

Kala will comply with the following 9 Data Protection Principles when processing personal data.

1. **Fairness and Transparency:** Kala will process personal data fairly and provide individuals with information about how and why their personal data is processed.

Kala will only hold data of individuals who have provided Kala with such information for the specific purpose for which it is provided. Kala will hold personal data of all members on the assumption that by payment of their annual subscription they are desirous of knowing and attending all Kala Events, Subscriptions, Booklets and publications of whatsoever format

2. **Lawful Processing:** Kala will only process personal data, including sensitive personal data, lawfully where it has a valid basis for the processing.

Generally, personal data will not be processed without a legal ground. In the context of Kala, personal data are typically processed on the basis of:

- processing necessary for the legitimate interests pursued by Kala, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This ground may apply to the processing of the personal data of any third party data subjects whose personal data are provided by the individual;
- a legal obligation to which Kala is subject and where compliance with such obligation necessitates the processing of personal data by Kala;
- data subject's consent, where such consent is procured from the individual; and
- other legal grounds.

3. **Purpose Limitation:** Kala will only collect personal data for a specific, explicit and legitimate purpose. Any subsequent processing should be compatible with that purpose, unless Kala has obtained the individual's consent or the processing is otherwise permitted by law.

Kala will typically process:

- the personal data of its members as required for the purposes of providing information regarding its various events and publications;

Kala will generally not carry out any unsolicited electronic marketing, but to the extent it does, it will have to comply with the law.

4. **Data Minimisation:** Kala will only process personal data that is adequate, relevant and limited to what is necessary for the purpose for which it was collected.

Kala will only obtain and retain such data is absolutely necessary for its functioning and for providing members with a quality user experience,

5. **Data Accuracy:** Kala will take reasonable steps to ensure personal data is accurate, complete, and kept up-to-date.

Kala may place a contractual obligation on each member or individual to ensure that any personal data provided in connection with the Kala services sought is accurate, complete and up to date.

Kala will endeavour to keep an accurate record of personal data in relation to its members and other individuals.



6. **Individual Rights:** Kala will allow individuals to exercise their rights in relation to their personal data, including their rights of access, erasure, rectification, portability and objection.

Kala will ensure that all individual Rights Requests are correctly identified and appropriately responded to, subject to any applicable exemptions.

7. **Storage Limitation:** Kala will only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.

Kala will keep all records as long as required by applicable law or as may be necessary having regard to custom, practice or the nature of the documents concerned.

Save for personal data included in records which must be kept for a prescribed period or preserved permanently in compliance with any legal obligations to which Kala is subject, such as the obligation explained above, personal data will be kept for no longer than necessary for the relevant purpose.

8. **Data Security:** Kala will use appropriate security measures to protect personal data, including where third parties are processing personal data on our behalf.

Kala will adopt the following security measures:

Physical security measures

- ensure physical security of premises, e.g. locked office;
- keep documents in locked cabinets;
- reduce access privileges to only those needed;
- grant access to only such persons who need to have access in connection with their duties;
- dispose of documents using a confidential bin or through a cross cut shredder; and
- other appropriate physical security measures.

Organisational security measures

- vet members and suppliers on a continuing basis;
- implement non-disclosure agreements prior to entering into formalised agreements;
- provide training to members where appropriate;
- implement a strict ban on the use of personal email for Kala purposes; and
- other appropriate organisational security measures.

Technical security measures

- firewalls where applicable will be properly configured and be using the latest software;
- regular patch management and OS updates will be implemented where applicable;
- real-time protection anti-virus, anti-malware and anti-spyware software where appropriate;
- user access control management
- unique passwords of sufficient complexity and regular (but not too frequent) expiry;
- data backup; and other appropriate technical security measures as appropriate

9. **Accountability:** Kala will take steps to comply with, and be able to demonstrate compliance, with the Data Protection Principles.

Kala will implement appropriate governance processes as set out in this Policy.

GOVERNANCE PROCESSES

In order to ensure that the Data Protection Principles are implemented Kala will adopt the following governance processes.



A. Documented Policies

In order to ensure compliance with Data Protection Principle 9 (Accountability), Kala will comply with this Policy and implement other relevant data protection policies and establish internal governance processes from time to time as may be required in order to operate Kala in compliance with data protection laws.

B. Assurance

Kala will ensure, by way of training or otherwise, that members carry out their tasks in a way that will ensure compliance with data protection laws. Each member and each Supplier shall have access to this policy and it shall have an obligation to comply with it.

Each supplier will have to comply with data protection obligations in accordance with its service agreement including, where appropriate, a data processing agreement.

Kala will periodically review this policy and other relevant policies to ensure that they continue to comply with the relevant legal requirements.

C. Advice

Where necessary Kala will seek advice in order to ensure that its processes comply with data protection laws.

D. Third Parties

Kala will comply with *this policy while appointing* any third-party contractor or supplier who will process personal data on behalf of Kala.

E. Data Protection Impact Assessments

Kala will implement a process so that any processing which is likely to result in a high risk to the rights and freedoms of individuals is subject to a documented Data Protection Impact Assessment (**DPIA**), to assess the risks associated with the proposed processing and identify any safeguards which should be put in place to mitigate those risks. Kala shall maintain a record of each DPIA.

F. Record-keeping

Kala will implement a process to maintain an up-to-date documented record of its processing activities by way of adding relevant information in the register or by other appropriate means. This record would include a general description of the following:

Record keeping requirements	Suggested record
<ul style="list-style-type: none">The purpose of the processing.	<ul style="list-style-type: none">Typically, in relation to transactions this will include processing to deliver client services;
<ul style="list-style-type: none">The categories of personal data and individuals to whom the data relates.	<ul style="list-style-type: none">A variety of mostly legal documents with copies of identity information relating to clients;
<ul style="list-style-type: none">The categories of recipients (if any), including both data controllers and data processors, and any transfers outside the European Economic Area (EEA).	<ul style="list-style-type: none">either the client or a third party to whom the client wished the documents to be sent after processing and such parties may often be located outside the EEA;
<ul style="list-style-type: none">Where possible, the envisaged retention period for the personal data.	<ul style="list-style-type: none">records will be retained in accordance with the Charity commission Rules; and
<ul style="list-style-type: none">Where possible, a general description of the technical and organisational security measures in place.	<ul style="list-style-type: none">the measures in place as set out at section 8 above.



Although it is envisaged that Kala will act as data controller in the majority of cases, where Kala processes personal data on behalf of another person, Kala will make sure to maintain a record of its activities as a data processor and/or data controller. This record will include a general description of the following:

- The identity of the individual and contact details.
- The categories of processing carried out on behalf of the third party.
- Any transfers outside the EEA.
- Where possible, a general description of the technical and organisational security measures in place.

G. Privacy by design

When implementing a new processing activity, tool or functionality involved in the processing of personal data, Kala will ensure, by contractual means or otherwise, that such activity, tool or functionality is designed and built in a way that allows Kala to comply with the Data Protection Principles.

H. Complaint handling

Kala shall implement a process to receive and handle enquiries and complaints from individuals and the supervisory authorities concerning the processing of personal data.

Kala shall ensure that all enquiries and complaints are dealt with in a timely manner, in compliance with any applicable statutory deadlines