KANTOS

Privacy Policy

Statement of intent

Kantos is committed to keeping all of your information safe and secure and to protecting your privacy. This privacy policy outlines how we will use data relating to website users, ticket purchasers, mailing list subscribers and our musician database. The policy may be updated so please check back to make sure that you're happy. By using our website or services you agree to be bound by this policy. If at any point you would like more information, or to be removed from one of our databases please get in touch: kantoschamberchoir@gmail.com

Personal Data We Collect

We collect and use different types of data, some of which is personally identifiable and some of which isn't. We collect data to report on our concerts and events, to help us communicate with musicians, colleagues and partners about opportunities and projects, and to improve our online communication. We only collect personal data that is essential to our operation as a charity, that promotes our work and enables us to fulfil our obligations to our stakeholders.

Statistical Data

We have access to analytics data from Instagram, Facebook, Twitter and MailChimp to gain insight into:

- The performance of our social media profiles, such as trends in reach.
- Our ad account's cross-platform spend.
- Organic and boosted post content engagement, including likes and comments.
- Demographic and geographic summaries of people who like our Page and follow our Instagram business profile.

Contact Data

If you message us on the 'Contact Us' section of our website (https://www.kantoschamberchoir.com/contact-us) we ask you to enter personal data in the form of your name, email address, and any message you would like to send to us. Your email address is collected so that we can get back in contact with you regarding your message. This information is not shared with any party other than necessary Kantos staff and volunteers.

Although we will endeavour to protect your data, we cannot guarantee its full security as no transmission over the internet is 100% secure. You therefore do this at your own risk.

Ticket Data

Where we sell tickets for our events directly, this is through Eventbrite. Orders will be processed through the Eventbrite system. We do not hold access to any information regarding payments made via Eventbrite. Where a concert is promoted through an external party we will use their ticketing system. In this instance you should refer to the Privacy Policy of the relevant venue.

We will not share data with an external 3rd party unless you have agreed to it, or to fulfil a requirement from a funder. In this instance we would anonymise your data.

KANTOS

Artist Data

When you sign up for a Kantos audition you consent for your data to be used by the choir to contact you. This data may include: name, email address, postal address, phone number and CV.

If you are successful in your audition you will be required to fill in a 'Personnel Details Form'. In addition to the above this will include: national insurance number, bank details, emergency contact information and, in the event of touring, passport and visa information. For the purpose of Kantos, all singers are responsible for their own self-employed financial reporting. Occasionally singer contact information may be passed on to third parties for professional opportunities. You will be given the opportunity to opt out of this as part of the 'Personnel Details Form'.

When singers sign up for an audition you will also be asked to fill in an equal opportunities form.

This data is held securely and can only be accessed by the Kantos Chamber Choir staff and volunteers for whom it is a relevant and necessary part of their job. We will only ask for information that is required. All sensitive files will be held securely and be individually password protected. Musician data is uploaded to our database on Google Drive, where all information is secured and encrypted.

Photos, Video and Audio Footage

Photos, video and audio are classed as personal information. For concerts, workshops and events we may photograph, video or audio record musicians. This is for marketing and publicity purposes. These photographs, audio and video recordings may be used in press, print, social media, on the Kantos website, or on the website of one of the Kantos partner organisations.

Audio or video footage collected as part of a professional engagement will become the property of the promoter. The musician will have received a fee in exchange for their services.

Your Rights

Under the General Data Protection Regulation (GDPR) anyone whose personal data is stored by Kantos has a set of rights relating to it. Those rights are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

If you would like to exercise one of these rights please let us know via kantoschamberchoir@gmailc.om

KANTOS

Review

A confidential record will be kept of any health and safety incidents, and this Policy will be reviewed annually, at our AGM, in the light of that record. If any have occurred, the nature of the incident and outcomes will be reviewed by the whole board, without disclosing confidential information. The whole Board of Trustees will make recommendations for changes to safeguarding procedures, including this policy in the light of any incidents. These may be made without waiting for the annual review.

Date 17/01/23

Signed

Chair of Trustees: Andrew Kyle

Managing Director: Claire Shercliff

KANTOS

Data Protection Impact Assessment (DPIA)

The following risk assessment has been used to support the writing of this policy.

Data protection issue	Mitigation measures	Conclusion
Purpose specification Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	- Specify/document the purposes for which personal data will be collected/used -Raise awareness of Kantos Privacy Policy that provides clarity on the purpose of data collection. -Improve training of staff regarding appropriate collection of data	Risk sufficiently mitigated
Data limitation Is all the personal data collected necessary for Kantos' activity? When people engage with the organisation, are they told how the personal information they supply will be used?	- Ensure staff collects only the pieces of data which are necessary to achieve the purpose specified originally - If possible, give people prior notice regarding the modalities/purposes of the data collection and processing. -Give individuals an opportunity to question the manner and purpose for which their data is collected and processed.	Risk sufficiently mitigated
Right to information Are individuals explicitly informed about why their personal data is being collected and how it may be used?	- Privacy policy displayed on Kantos' website	Risk sufficiently mitigated

KANTOS

<u>Legal basis for data processing/transfer</u> <u>Consent</u> Are individuals able to appreciate the most likely consequences (including negative)? Does the person have a genuine free choice as to whether to consent? Are they able to refuse to provide some or all information without being penalised in any way or deprived of any service your organisation might otherwise provide? How do individuals provide consent for their information to be collected? If consent is not written, do you see any risks involved? Is consent limited to a specified purpose? If the personal data were to be used for a purpose other than that originally specified (a secondary purpose), will a new consent be sought from the individual? Has the individual explicitly agreed to how their information can be used, or that it can be shared with other agencies? Are there instances or circumstances where an individual has consented to the sharing or disclosure of personal information, but where the staff in charge does not think it is	- Review the process by which consent is sought. Explain to artists/collaborators the implications of Kantos holding data, how their data could be used in the database and to whom it could be further transferred. e.g. possibility of passing information onto third parties for additional work opportunities. - Attempt, where possible, to get a signed informed consent form/contract. - Ensure that the consent form is consistent and accessible across all methods of collection, including hard-copy/online forms and via telephone. -If it is not possible to obtain an informed consent: process/transfer personal data on an alternative legal basis (vital interest , public interest , legitimate interest, compliance with a legal obligation)	Risk not necessarily mitigated but accepted

wise to do so? <u>Alternative legal basis</u> Is data also collected of individuals who are not present?		
<u>Right to access / Rectification / Deletion</u> Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information? Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	- Rights outlined in Privacy policy published on website with relevant contact details for action	Risk sufficiently mitigated
<u>Appropriate security measures</u> What personal information is to be collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity, religion, sexual orientation, political views, trade union membership, etc.) Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to	- Develop robust access control protocols which limit access on a 'need to know' basis. - Users should only have access to that portion of data they need to carry out their legitimate functions. - Access to databases is only granted to those working within the organisation. - Ensure clarity re who has the authority to assign, change or revoke access privileges. - Set-up data breach notification procedures to inform the data subjects.	Risk not necessarily mitigated but accepted

surveillance? What preventative measures are in place? Does the processing involve external organisations or third parties? Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a “need to know” basis? How is this implemented in practice? Is training given to all staff on good data protection and information security practices? What action will be taken if there is a data breach? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organisations be informed? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organisation was compromised or deleted either by accident or purposely? How would you decide which risks are the most likely and those that are likely to have the greatest impact if the personal		

information were stolen, hacked, altered or stolen?		
<u>Data retention</u> Is personal information being entered into databases? Is it necessary to keep all of the data that is being processed? Are there procedures for reviewing how long data should be retained?	- Limiting the retention of personal data to what is necessary to fulfil specific, explicit and legitimate purposes. - Use of database: As part of a privacy-by-design approach, ensure the data retention period is considered - link the data retention period to the purpose of the data processing operations. An initial retention period could be extended if it is considered necessary to keep the data to fulfil the purpose for which it was originally collected.	Risk sufficiently mitigated