Looe Festival of Words (LFOW) GDPR POLICY DOCUMENT

LFOW keep the following List of Information:

- Names, addresses, email addresses, and phone numbers of contributors
- Names and contact details of steering group members
- Names and contact details of volunteers

Our Lawful Basis for keeping the information is:

1. **Legitimate Interest**
- To organise events for the festival and update contributors and volunteers on such
- For request feedback for planning future festivals
- To send out publicity for this year's festival and future ones
- In order to prioritise applications for bookfair as the festival has the stated aim as being focussed on South East Cornwall

2. **Consent**
- We have consent from those who send the information

How we keep this information securely:

- On a secure (encrypted) database
- With managed access limited only to members of the festival steering group

Our Transparency Notice:

Looe Festival of Words staff / volunteers privacy notice

This privacy notice tells you what to expect us to do with your personal information when you work for us.

Contact details

Email: looefestivalofwords2024@outlook.com

What information we collect and use, and why

Staff and volunteer recruitment, administration and management

*We collect or use the following personal information as part of **staff and volunteer recruitment, administration and management**:*

- *Contact details (eg name, address, telephone number or personal email address)*

*Our lawful bases for collecting or using personal information as part of **staff recruitment, administration and management** are:*

- *Consent*
- *Legitimate interest:*

• To organise events for the festival and update contributors and volunteers on such • For request feedback for planning future festivals • To send out publicity for this year's festival and future ones • In order to prioritise applications for bookfair as the festival has the stated aim as being focussed on South East Cornwall

Where we get personal information from

We collect your information from the following places:

- *From staff members or volunteers directly*

How long we keep information

2 years

Your data protection rights

Under data protection law, you have rights including:

***Your right of access** - You have the right to ask us for copies of your personal data.*

***Your right to rectification** - You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.*

***Your right to erasure** - You have the right to ask us to erase your personal data in certain circumstances.*

***Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal data in certain circumstances.*

***Your right to object to processing** - You have the right to object to the processing of your personal data in certain circumstances.*

***Your right to data portability** - You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances.*

***Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent.*

You don't usually need to pay a fee to exercise your rights. If you make a request, we have one calendar month to respond to you.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

Website: https://www.ico.org.uk/make-a-complaint

Last updated

30 June 2024

How We Will Deal with a Request for Information (Process):

By law, people can ask you for a copy of any information that's to do with them. It might be saved on our system, but if it's about them, it's their personal data, and they have a right to see it. If they ask us for a copy of it, by phone, in person, or in writing, they have made a 'subject access request' (SAR), and we need to take action.

1. Data Protection Lead: [NAME] will respond:
2. Checking the Requestor's ID (by asking something only they would know – what?)
3. Checking the Request is Valid: if not made by the person themselves, that they have written authority from that person or Lasting Power of Attorney for them.
4. Information will be sent within ONE CALENDAR MONTH
5. Only send the data requested and nothing more
6. Replies will be sent by email (as requested by email)

How We Will Handle Breaches of Personal Data:

If any personal information we're responsible for is lost, accidentally destroyed, altered without proper permission, damaged or disclosed to someone it shouldn't have been, this could be a personal data breach. This could be as a result of a cyber-attack, flood, fire or theft, perhaps an email has been sent to the wrong person, a laptop was stolen from a car.

Where this happens, we will act quickly and we may need to report it to us [ICO] within 72 hours.

- **Start the timer:** By law, we've got to report a personal data breach to the ICO without undue delay (if it meets the threshold for reporting) and within 72 hours. We will log it anyway.
- **Find out what's happened:** We will log the facts – what happened and why, names of those involved, timeline of when it happened, actions we've taken
- **Try to contain the breach:** Our priority is to establish what has happened to the personal data affected. If we can recover the data, we will do so immediately. We will also do whatever we can to protect those who will be most impacted.
    - If it's been sent to someone by mistake, we could ask them to delete it, send it back securely, or have it ready for us to collect.

    - If we don't know where it is, we will retrace our steps. If we think it's been lost in an office or building, we could try calling the reception.
    - If we're dealing with a stolen laptop and we've got the appropriate systems installed, we will wipe it remotely. This will help to minimise the risk of personal data falling into the wrong hands.
    - We could contain a cyber incident by changing all passwords and making sure our staff and volunteers do the same.
    - If we need help thinking of other ways to contain the breach, we can contact ICO to advise us.
- **Assess the risk:** of harm to those affected, i.e. any potential harm or detriment it may cause to people, e.g. safeguarding issues, identity theft or significant distress. We might be dealing with a simple mix-up where there's little or no risk involved, or a serious breach that will have a lasting effect on people's lives.
- **If necessary, we will act to protect those affected:**
    - Depending on the circumstances, this may include advising people to use strong, unique passwords, telling them to look out for phishing emails or fraudulent activity on their accounts and providing guidance on protecting themselves from identity theft.
    - We may tell people about the incident, even if we don't think there's a high risk to them, but we will want to balance any risk to them against the potential of causing unnecessary worry.
    - If we think there's a high risk, then by law we have to tell them without undue delay. For example, if we feel there is a high risk of them having their identity stolen, then we have to let them know so they can be extra vigilant and take steps to protect themselves.
- **Submit your report (if needed):** If the breach is reportable, we can report it online, using our the ICO self-assessment tool or calling the ICO personal data breach advice line on 0303 123 1113 to help decide if it is reportable.

Registration with the ICO (Information Commissioners Office):

£40 but having completed the ICO self assessment tool, we come up as exempt.

Reminders:

Review GDPR Policy annually at Steering Group Meeting