



## **FRIENDS OF LEWES**

**Registered charity 258756**

### **DATA PROTECTION & PRIVACY POLICY**

**The Friends of Lewes (FoL) collects and uses certain types of information about the individuals it encounters in the course of its activities and the delivery of the services it provides.**

The purpose of this policy is to outline how FOL processes such information in line with the provisions of the UK General Data Protection Regulation and the Data Protection Act 2018 and other relevant legislation.

#### **1. UK General Data Protection Regulation and Data Protection Act 2018**

The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) are designed to ensure that personal data about living individuals is handled properly by organisations and that the rights of individuals to access information that is held about them are protected.

#### **2. What is personal data?**

Personal data is information about a living individual from which that person can be identified. Such information can exist in a variety of formats, for example, on a computer or in a paper filing system.

#### **3. What principles apply to the collection of personal data?**

There are eight governing principles that must be followed in connection with the processing of data about individuals. These state that information must:

- a) Be processed fairly and lawfully.
- b) Be collected and processed for the particular purposes specified. In other words, it must not be collected for one reason and then used for another.
- c) Be adequate, relevant and not excessive for the purposes for which it is kept.
- d) Be accurate and, where necessary, kept up to date.
- e) Not be kept for longer than necessary.
- f) Be processed in accordance with the subject's rights.
- g) Be kept securely and adopt measures to guard against its accidental loss.
- h) Not be transferred outside the U.K unless the country receiving it has an adequate level of protection for the rights and freedoms of data subjects.

#### **4. How we use personal data**

All personal data is treated strictly in accordance with the terms of the UK GDPR and DPA 2018.

This means that, as outlined below, confidentiality will be maintained, and appropriate security measures are taken to prevent unauthorised disclosure.

When members join the Friends of Lewes (FoL), they are asked to provide their name, postal address, email address (if any) and a contact telephone number. FoL also keeps a record of membership payments.

Those who simply want to be kept informed of relevant events and news by email can enrol on our website and manage their own enrolment via a link at the bottom of every such email.

We use personal details only for FoL-related purposes, and do not divulge them to any third party without prior consent. We explain to each member why we ask them for the information and assure them that it will be carefully managed. We ask for all members to agree to FoL holding their personal details on paper and electronically and maintain a record of this agreement. We also point out where our full Data Protection and Privacy Policy can be found.

The explanation and the precautions taken to manage the data are found on Friends of Lewes website under Data Protection.

#### **5. What personal data is used for**

We use the data to communicate with our members and followers by email, post and – very occasionally – telephone for urgent contact. Our policy is to use email BCC (blind copy) features to ensure that members' details are not disclosed to others unless they have given prior consent, for example when a group of members is working together on a project.

It is the responsibility of a member to make it clear that they are resigning from FoL to prevent further communications.

Members who have not renewed their membership within the due period specified in FoL's constitution will be removed from the list of members. An attempt will be made to contact the member at their last known postal or email address, letting them know that they will be deleted from the FoL membership database.

#### **6. Lawful basis for holding personal data**

Our lawful basis for holding our members' personal data is consent, that is the consent given on the membership application when a person becomes a member or renews their membership.

Any individual about whom FoL holds personal data will be given access to the data held about them on request and can ask for it to be deleted (although that would effectively terminate their relationship with FoL). At all times, FoL will ensure that the rights of individuals can be fully exercised. If unsatisfied, individuals have the right to complain to the supervisory authority and to a judicial remedy.

#### **7. How the data is protected**

Member data is managed and controlled by the Membership Secretary, under the direction of the Secretary, who is a member of the FoL Executive Committee.

To ensure data security, we take the following steps and policies:

- We have a Data Protection Officer, who sits on the Executive Committee and is responsible for ensuring compliance with data protection legislation.
- We have a membership secretary whose role encompasses managing memberships and routine communications. Email communications with the membership are undertaken by the Web Manager.
- The original (hardcopy) membership and renewal application forms are securely and methodically stored by the Membership Secretary.
- The membership database is hosted by Membermojo and maintained by the Membership Secretary on a PC with current levels of operating system software, anti-virus and anti-malware software.
- The membership database is password protected and encrypted.
- The membership database is backed up regularly, and the back-up is held on a secure cloud storage.
- The password to the digital membership database is known only to the Membership Secretary, the Executive Committee Secretary and the Website Manager.
- Access to managing our website is also password controlled, with access limited to the Website Manager and one E.C member.
- Access to managing our social media services (Facebook) is also password controlled, with access limited to the Website Manager and two E.C members.

Should our data or other digital assets be hacked, we would advise members of what occurred, investigate the breach and take steps to prevent its recurrence. The Membership would also be advised of what actions they should take including changing their passwords.

## **8. Review**

This privacy notice will be reviewed periodically by the executive committee to reflect best practice in response to changes in relevant legislation or an identified failing in its effectiveness.

It is the opinion of the Data Protection Officer that our privacy policy offers sufficient security and privacy for a volunteer non-profit group of our size, purpose and activities.