FOAF Data Protection Policy

Acknowledgement: This document is based on one for Warwick District U3A, which is in turn modelled on a sample document from Third Age Trust, the governing body of the U3A in the UK.

SCOPE OF THE POLICY

This policy applies to the work of Friends of Abbey Fields (hereafter 'FOAF'). The policy sets out the requirements that FOAF has to gather personal information for membership purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the FOAF committee members to ensure that FOAF is compliant. This policy should be read in tandem with FOAF's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that FOAF:

- Complies with data protection law and follows good practice
- Protects the rights of members
- Is open about how it stores and processes members' data
- Protects itself from the risks of a data breach

GENERAL GUIDELINES FOR COMMITTEE MEMBERS AND GROUP CONVENORS

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to the members of FOAF
- Data should not be shared informally or outside of FOAF
- FOAF will provide induction training to committee members to help them understand their responsibilities when handling personal data
- Committee Members should keep all data secure, by taking sensible precautions and following the guidelines below
- Strong passwords must be used and they should never be shared
- Personal data should not be shared outside of FOAF unless with prior consent and/or for specific and agreed reasons
- Member information should be reviewed and consent refreshed periodically via the membership renewal process or when policy is changed

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies eight data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary

Principle 6 - Personal data must be processed in accordance with the individuals' rights

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Lawful, fair and transparent data processing
FOAF requests personal information from potential members and members for the purpose of sending communications about their involvement with FOAF. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. Members will be asked to provide consent for their data to be held and a record of this consent along with member information will be securely held. FOAF members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a FOAF member requests not to receive certain communications this will be acted upon promptly and the member will be informed as to when the action has been taken.

Processed for Specified, Explicit and Legitimate Purposes
Members will be informed as to how their information will be used and the Committee of FOAF will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about FOAF's events and activities
- Communicating with members about their membership and/or renewal of their membership
- Communicating with members about specific issues that may have arisen during the course of their membership
- Communicating with members about occasional local events which may be of interest

FOAF will ensure that committee members are aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending FOAF members marketing and/or promotional materials from external service providers.

FOAF will ensure that members' information is managed in such a way as to not infringe an individual members rights which include:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Adequate, Relevant and Limited Data Processing
Members of FOAF will only be asked to provide information that is relevant for membership purposes. This will include:

- Name.
- Postal address.
- Email address.
- Telephone number.
- Gift Aid entitlement.

There may be occasional instances where a member's data needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the member or FOAF in those instances where FOAF has a substantiated concern then consent does not have to be sought from the member.

Accuracy of Data and Keeping Data up to Date
FOAF has a responsibility to ensure members' information is kept up to date. Members will be informed to let the membership secretary know if any of their personal information changes. In addition, on an annual basis the membership renewal forms will provide an opportunity for members to resubmit their personal information and reconfirm their consent for FOAF to communicate with them.

Accountability and Governance
The FOAF Committee is responsible for ensuring that FOAF remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The FOAF Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within FOAF and the reasons for this. The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

Secure Processing
The committee members of FOAF have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members using strong passwords.
- Committee members not sharing passwords.
- Restricting members' information to those on the Committee who need to communicate with members on a regular basis.
- Using password protection on laptops and PCs that contain or access personal information.
- Using password protection or secure cloud systems when sharing data between committee members and/or group convenors.
- Paying for firewall security to be put onto Committee Members' laptops or other devices if necessary.

FOAF has contracted for services with Emmerson Press for printing of our newsletter, but no personal data is passed to them.

Subject Access Request
FOAF members are entitled to request access to the information that is held by FOAF. The request needs to be received in the form of a written request to the Membership Secretary of FOAF. On receipt of the request, the request will be formally acknowledged and dealt with within 14 days unless there are exceptional circumstances as to why the request cannot be granted. FOAF will provide a written response detailing all information held on the member. A record shall be kept of the date of the request and the date of the response.

Data Breach Notification
Were a data breach to occur, action shall be taken to minimise the harm by ensuring all committee members are aware that a breach had taken place and how the breach had occurred. The committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of FOAF, in liaison with committee members, will assess the severity of the breach and if deemed serious enough, the Information Commissioner's Office would be notified. The committee shall also contact the relevant FOAF members to inform them of the data breach and actions taken to resolve the breach.

If a FOAF member contacts FOAF to say that they feel that there has been a breach by FOAF, a committee member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the committee member will ask the FOAF member to follow this up with an email or a letter detailing their concern. The concern will then be investigated by members of the committee who are not in any way implicated in the breach. The FOAF member should also be informed that they can report their concerns to the Information Commissioner if they don't feel satisfied with the response from FOAF. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.