Friends of Eastfield Park

Data Protection Policy

1. Introduction

In order to meet its objectives, 'Friends of Eastfield Park' (FoEP) needs to collect and use certain types of information about many of the people we have contact with. This personal information must be collected and dealt with appropriately - whether on paper, in a computer, or recorded in some other way - and there are safeguards to ensure this happens under the Data Protection Act, 1998.

The following list defines the technical terms used in this document:

Data Controller: The person(s) who decides what personal data the FoEP will hold and how it will be held or used.

Data Protection Act, 1998: The UK legislation that provides a framework for responsible behaviour by those using personal data.

Data Protection Officer: The person(s) who ensure that the FoEP follows its data protection policy and complies with the Data Protection Act, 1998.

Data Subjects: The individuals whose personal information is being held or processed by the FoEP (e.g. supporters and volunteers).

'Explicit' consent: is freely given, specific and informed agreement by a Data Subject to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification: Notifying the Information Commissioner about the data processing activities of the FoEP. Certain activities may be exempt from notification.

Information Commissioner: The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing: means collecting, amending, handling, storing or disclosing personal data.

Personal data: Information about living individuals that enables them to be identified, e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual supporters of the FoEP.

Sensitive data: means information about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings

2. Data Controller

The FoEP is the Data Controller under the Act, which means that it determines what personal information will be collected, how it will be held, and what it will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Although the FoEP will usually keep personal data about its supporters (including name, address, phone number and email address and, possibly, occupation, place of work, position held, membership of other organisations, skills, interests and date of birth) it will not, without seeking special permission from the FoEP committee and the Data Subjects, hold any sensitive data.

3. Disclosure

The FoEP may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

In most circumstances the Data Subject will be made aware how and with whom their information will be shared. There are circumstances where the law allows the FoEP to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State,
2. Protecting vital interests of a Data Subject or other person,
3. The Data Subject has already made the information public,
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights,
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion,
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

4. Data Protection

The FoEP regards the lawful and correct treatment of personal data as very important to its successful working, and to maintaining the confidence of those with whom we deal.
The FoEP intends to ensure that personal information is treated lawfully and correctly.
To this end, the FoEP will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s),
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The FoEP will, through appropriate management and strict application of criteria and controls:

1. Fully observe conditions regarding the fair collection and use of information,
2. Meet its legal obligations to specify the purposes for which information is used,
3. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
4. Ensure the quality of information used,
5. Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong
6. Take appropriate technical and organisational security measures to safeguard personal information,
7. Ensure that personal information is not transferred abroad without suitable safeguards,
8. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
9. Set out clear procedures for responding to requests for information.

5. Data collection

Informed consent is given when a Data Subject clearly understands why their information is needed, who it will be shared with and the possible consequences of them agreeing or refusing the proposed use of the data, and then gives their consent.

The FoEP will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, the FoEP will ensure that, as far as is reasonably practicable, the Data Subject:

1. Clearly understands why the information is needed,
2. Understands how the information will be used and the possible consequences of refusing consent,
3. Grants consent, either written or verbally, for the data to be processed,
4. Is competent to give consent and has given so freely without duress,

6. Data Storage

Information relating to supporters will be stored securely and will only be accessible to committee members and authorised volunteers.

Information will be stored for only as long as it is needed and will be disposed of appropriately.

It is FoEP's responsibility to ensure all personal data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

7. Data access and accuracy

All Data Subjects have the right to access the information the FoEP holds about them. The FoEP will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, the FoEP will ensure that:

1. It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection,
2. Everyone processing personal information understands that they are responsible for following good data protection practice,
3. Everyone processing personal information is appropriately trained to do so,
4. Anybody wanting to make enquiries about handling personal information knows what to do,
5. It deals promptly and courteously with any enquiries about handling personal information,
6. It describes clearly how it handles personal information,
7. It will regularly review and audit the ways it holds, manages and uses personal information,
8. It regularly assesses and evaluates its methods and performance in relation to handling personal information,
9. All committee members are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any amendments made to the Data Protection Act 1998.

In case of any queries in relation to this policy please contact the Data Protection Officer.

The current Data Protection Officer is: Vic Smith

Approved by the FoEP Committee: January 2013 (to be confirmed)

Agreed / Revised at the FoEP AGM on: 18th February 2013