****

**Introduction**

The Friends of Sussex Hospices needs to keep certain information about its volunteers and supporters to run the charity. It is also necessary to process information so that FSH can comply with its legal obligations and organise volunteers. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, FSH must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 ACT).

In summary these state that data shall:

Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose

Be adequate, relevant and not excessive for that purpose

Be accurate and kept up to date

Not be kept longer than is necessary for that purpose

Be processed in accordance with the data subject’s rights

Be kept safe from unauthorised access, accidental loss or destruction.

Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

FSH and others who process or use personal information must ensure that they follow these principles at all times.

In order to ensure that this happens, FSH has developed this Data Protection Policy and the accompanying Data Protection Code of Practice.

**Status of this Policy**

This policy does not form part of a formal offer of a position for volunteers but it is a condition of volunteering that volunteers will abide by the rules and policies made by FSH from time to time.

**The Data Controller and the Designated Data Controllers**

FSH as a charity is the Data Controller under the 1998 Act and the Trustees are ultimately responsible for implementation. However, the Designated Data Controller(s) will deal with day to day matters. The Data Controller is the Minutes Secretary.

Any volunteer or other individual who considers that the Policy has not been followed in respect of personal data about him or herself should raise the matter with the Designated Data Controller.

**Volunteer Obligations**

Volunteers must ensure that all personal data provided to FSH is accurate and up to date, eg contact address

Volunteers who may, from time to time, process personal data must comply with the guidelines for data collection and security as set out in FSH’s Data Protection Code of Practice.

**Data Security**

All volunteers are responsible for ensuring that:

Any personal data is kept securely

Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Personal data should:

Be kept in a locked filing cabinet, drawer or safe

If computerised, be coded, encrypted or password protected both on a hard drive or on a network drive that is regularly backed up and

If a copy is kept on a diskette or other removable storage media, that media must themselves be kept in a locked filing cabinet, drawer or safe.

**Rights to Access Information**

All volunteers and supporters are entitled to:

Know what information FSH holds and possesses about them and why.

Know how to gain access to it

Know how to keep it up to date

Know what FSH is doing to comply with its obligations under the 1998 Act.

This Policy document and FSH’s Data Protection Code of Practice address in particular the last 3 points above. To address the first point, FSH will, upon request, provide all volunteers and supporters with a statement regarding the personal data held about them. This will state all the types of data which FSH holds about them and the reasons for which they are processed.

All volunteers and supporters have a right under the 1998 Act to access certain personal data being kept about them either on a computer or in certain files. Any person who wishes to exercise this right should submit a request to the Designated Data Controller.

FSH aims to comply with such requests within the 40 days provided by the 1998 Act.

**Publication of Information**

The names of Senior Officers and Trustees of FSH or any other personal data relating to Trustees will be published in the annual report and on the public web site when any statute or law requires such data to be made public.

It may be the case that volunteers may produce web-based material containing personal data. All such activities are set out in detail in FSH’s Data Protection Code of Practice.

**Retention of Data**

FSH has a duty to retain some volunteer personal data for a period of time following their departure from FSH. The exact details are set out in Annex 1 to FSH’s Data Protection Code of Practice.

**Conclusion**

Compliance with the 1998 Act is the responsibility of all members of FSH. Any deliberate breach of the Data Protection Policy could lead to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Controller.

**DATA PROTECTION CODE OF PRACTICE**

**Introduction**

This CoP must be read in conjunction with FSH’s Data Protection Policy document to give the fullest picture of FSH’s data protection regime. This document gives and introduction to some basic points of practice relating to the handling and processing of personal data at FSH. It also lists the particular activities carried out within FSH which involve the handling and processing of personal data.

**Key Concepts**

The 1998 Act places an obligation on FSH, as a data controller, to collect and use personal data in a responsible and accountable fashion. FSH is committed to ensuring that every current registered volunteer complies with the Act to ensure the confidentiality of any personal data held by FSH in whatever medium. Three key concepts to be considered are: purpose, fairness and transparency.

**Purpose**

Data controllers can only process personal data where they have a clear purpose for doing so, and then only as necessitated by that purpose. Annex 3 of this CoP summarises the purposes for which FSH processes personal data. Personal data cannot be processed for purposes that have not been defined and declared in FSH’s Data Protection Register entry (see below).

**Fairness**

In defining the purposes for which FSH processes personal data, the fairness of that processing must be considered. For some types of processing the required elements of fairness and legality are outlined in the legislation but for many others they are not. In such cases, FSH has tried to take a broad approach to deciding what is fair in each case, based on an interpretation of the 1998 Act and in conjunction with the advice from the Information Commissioner and on wider practice within the UK charity sector.

**Existing Notifications**

The Act requires many data controllers to notify the Information Commissioner of the purposes for which personal data are processed, together with certain details of that processing. Those notifications are then held on a public register.

It is an offence for FSH to hold personal data that falls outside the classes declared in these notifications or to process personal data for any purposes that are not defined there. It is very important that those who work with personal data in FSH are familiar with the details contained in these notifications.

**Collection of personal data**

In most cases, the personal data held by FSH will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Anyone responsible for managing the collection of personal data for the legitimate activities of FSH must ensure that a notice containing the following information is included in the request for that data:

(a) A statement that FSH, is the data controller

(b) The name and or job title of the specific individual responsible for the administration of the personal data being collected, to enable, for example, subsequent amendments to be submitted by the data subject

(c) A clear explanation of the types of data being collected and the purposes for which that data will be processed

(d) Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed

(e) A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place

**Amendment of personal data**

From time to time, data subjects will wish to update some of their personal data held by the Data Controller, for example their home addresses or other contact details previously submitted. To do this, the data subjects must contact the Designated Data Controller.

**Security of personal data**

Of fundamental importance within any data protection regime is the security of the personal data being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside FSH.

Authorised disclosures or transfers are those that are defined within the appropriate Notifications and declared to the data subject either at the point of data collection or subsequently; the necessary consent for disclosure or transfer having been obtained if required.

**Disclosures outside FSH**

When a request to disclose or amend personal data relating to a data subject is received from an individual or organisation outside FSH, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established.

Requests for the disclosure of personal data from the Police, Government bodies, the British Council or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given.

**Publication of Information**

Whilst the majority of personal data held by FSH is processed for internal administrative purposes and is never disclosed outside the organisation, some categories of data are routinely or from time to time released through one or more forms of publication.

**Legal Obligations**

When required by law or statute, the names of senior officer and trustees of FSH and certain other personal data relating to trustees are published in the annual AGM report and on the website. FSH also fulfils all obligations placed upon it by its relationship with various funding bodies.

**Volunteer personal data on web pages**

Apart from obligations mentioned above, FSH will not ordinarily reveal any personal details of FSH volunteers or supporters to any individual or body outside FSH.

**Disposal of personal data**

All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed by re-formatting, over-writing or degaussing

All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating.

Volunteers will be provided with guidance in the Volunteer Handbook as to the correct mechanisms for disposal of different types of personal data

In particular, volunteers will be made aware that erasing/deleting electronic files does not equate to destroying them.

**Subject Access Requests**

All volunteers have a right to access certain personal data being kept about them at FSH. Any person who wishes to exercise this right should submit the application to the Data Controller.

Annex 1–

**Purposes for which Personal Information may be held and processed**

FSH processes personal information to enable it to:

Provide a voluntary service for the benefit of the public

Administer membership records

Fundraise and promote the interests of the charity

Manage volunteers

Maintain its own accounts and records