Forest Voluntary Action Forum (FVAF)

Data Protection, Handling and Management Policy

1. Background

Most data held by FVAF is about organisations, their staff and volunteers. Data protection legislation relates to personal data, about identifiable people, and organisations by definition cannot be data subjects, covered by the regulations. Named contacts within organisations do however qualify. Home addresses used as contact points for organisations, even if a name is not held, could be viewed as making it possible to identify an individual and it would therefore be wise to treat this as personal data.

Explicit consent by the individual is not likely to be required for uses such as mailing lists used by FVAF, to keep notes on client case work, membership records or other services supplied. It would be good practice to inform them of likely use when the data is first collected. Such uses should be part of a Data Protection notification (to the Information Commissioner), although some may be borderline re exemptions. Publishing a directory, in print or on the web, is likely to go beyond the necessary 'legitimate interests' and consent should be sought.

Volunteering and personal services

Records used in these areas of work will relate to individuals. Some of the data is likely to fall within the definitions of 'sensitive' data, where further requirements must be met – see Appendix. Usually explicit consent of the individual is required. Recording for monitoring purposes does not require this, if it is on ethnic or racial origin, disability or religion. Confidential counselling, advice, support or other (similar) services do not need consent if it cannot be obtained or it is reasonable to proceed without it. Records on offenders deemed unsuitable to work with certain client groups are likely to need specific clarification.

2. Notification and responsibility

FVAF will ensure that it conforms with Notification requirements under the Data Protection Act, and, as a Data Controller, renewing any notification and updating uses as appropriate.

The Manager will ensure that this policy and related procedures are understood and adhered to by FVAF staff and volunteers.

3. Data collection, recording and use

All data, whether falling under Data Protection legislation or not, will be obtained, processed and used fairly and lawfully, in accordance with the principles of good practice of the Data Protection Act.

In respect of the Volunteer Centre explicit consent should be obtained for recording any information on health or criminal matters concerning individuals where this is necessary in terms of managing volunteering services. Prospective volunteers should be informed of the reasons for such records being made. As good practice, individuals will be informed if religion or ethnicity data is recorded for monitoring purposes.

Should FVAF offer any direct services in the future then explicit consent should be obtained for recording any information on health or criminal matters concerning individuals where this is necessary in terms of managing services. Service users should be informed of the necessity of such records to be able to provide an effective service. As good practice, individuals will be informed if religion or ethnicity data is recorded for monitoring purposes.

Work on organisational development or similar will only record sensitive data such as religion, ethnicity or disability for monitoring purposes in respect of an organisation's client group or membership. Such information will not be held for individual contacts for organisations.

All organisations or individuals whose details are to be recorded will be informed of the intended use of this data.

Any intended use beyond the normal functions of a volunteering and voluntary sector development agency must be agreed by all parties to any data sharing arrangement, in respect of the data concerned.

4. Data accuracy and retention

Procedures will be established to ensure changes in contact data are captured and actioned in a timely and effective manner. Priority will be given to corrections to any inaccurate or out-of-date personal data.

5. Security

Adequate procedures will be put in place to prevent unauthorised access to data, whether held on computer or manually. Steps will be taken to avoid accidental loss or damage of data, such as back-up systems, off-site storage.

6. Rights and disclosure

Organisation data, excluding personal details, may be disclosed to agreed types of organisation, such as statutory agencies or relevant voluntary bodies. Personal data of individual contacts will only be disclosed, including in a published directory or website listing, with prior consent.

Volunteers or service users will not be sent marketing material other than information directly related to the service provided by FVAF.

Individuals may request a record of any personal data held by the organisation. Replies should be given within 2 weeks and full details within a month. No fee would normally be charged.

Staff will not withhold information from their line manager unless it is purely personal.

September 2013

Appendix - Data Protection Principles, Definitions

Extracts from Data Protection Legal Guidance. See Information Commissioner's website at www.informationcommissioner.gov.uk for full document and further details.

The eight principles of good practice
Anyone processing personal information must comply with eight enforceable principles of good information handling practice.
These say that data must be:
1. fairly and lawfully processed (see six conditions below)
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the individual's rights
7. secure
8. not transferred to countries outside European Economic area unless country has adequate protection for the individual.

The six conditions (derived from Schedule 2 of DPA). At least one of the following conditions must be met for personal information to be considered fairly processed:
1. the individual has consented to the processing
2. processing is necessary for the performance of a contract with the individual
3. processing is required under a legal obligation (other than one imposed by the contract)
4. processing is necessary to protect the vital interests of the individual
5. processing is necessary to carry out public functions, e.g. administration of justice
6. processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

Sensitive personal is personal data consisting of information as to the persons :

a. racial or ethnic origin of the data subject,
b. political opinions,
c. religious beliefs or other beliefs of a similar nature,
d. membership of a trade union,
e. physical or mental health or condition,
f. sexual orientation,
g. commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in such proceedings.

Processing of sensitive personal data must meet additional conditions which includes explicit consent