

## **VOLUNTARY ACTION – LEEDS**

### **DATA PROTECTION POLICY**

Voluntary Action – Leeds takes seriously its obligations under the Data Protection Act 1998, and we are registered with the Information Commissioner. Our registration, which is renewed annually, allows us to process certain personal information following very strict guidelines, which define the data subjects, the classes of data, which may be held, and the data recipients. We hold data for the purposes of Staff Administration, Membership Administration, Fundraising and Realising our Charitable Objectives. Personal data is defined as *information about a living individual who is identifiable by that information, or who could be identified by the information combined with other data; it includes recorded opinion about or intentions regarding a person*. The data falls into two main categories:-

- (a) staff data (VA-L employees)
- (b) external data

#### **(a) Staff Data**

##### What

Various data is held on staff relating to their employment with Voluntary Action – Leeds: this will cover all aspects of recruitment, selection and employment such as the job application form, interview assessments, references, probationary and annual reviews and supervisions, bank details and national insurance number, details of any deductions from pay (e.g. to the courts...or to trades unions), sick notes and medical assessments, details of grievance and disciplinary proceedings including current warnings (within the timescale allowed by the appropriate policies), reference requests, etc. Much of this data is, by its nature, highly personal, and Voluntary Action – Leeds recognises that it is its duty to safeguard the data by all possible means, and to notify staff about what is kept and why, along with information on how the data can be accessed and by whom.

## Why

The data kept on staff is exclusively in relation to their employment with Voluntary Action – Leeds; no unrelated data will be kept. The data that is kept will be used for the purpose of administering and managing the employment.

## Where

Most personal data is kept in individual personnel files in the Administration Manager's office and these are locked. Other data (e.g. bank details, n.i. number, deductions details) are kept by the Payroll Department, and again these are kept locked. Line managers also keep staff files covering supervision sessions plus any job-related information necessary for management. Again, these are kept locked. Computer files (e.g. supervision records, payroll details) are passworded and secured.

## Whom

All staff contracts include information on data protection, and make clear that by signing the Statement of Written Employment Particulars, staff give consent for VA-L to keep the data outlined above and to use it in the ways outlined above. Access to staff data is restricted to Management at the appropriate level, to Payroll staff for any issues specifically relating to pay, and to senior administrative staff (in connection with file maintenance, employment correspondence and the like). Staff are entitled to see their own personnel files; to do so, they should arrange a mutually convenient time with their line manager.

## How Long

Information on how long data is kept for can be found in VA-L's Archiving Policy which should be read alongside this Policy.

## I.T.

Personal data held on computers (including files, emails, databases, etc) and personal data downloaded from the web or posted on the web are subject to the same control and restrictions as paper-based data. Staff must take particular care when using any personal data in these contexts.

Staff should be aware that VA-L may monitor use of the internet and/or emails; further information on this may be found in the Statement of Written Employment Particulars, and in the Internet/Email Policy.

### Staff Obligations

While the General Manager is the Registered Data Controller, all staff are responsible for ensuring their compliance with this Policy – for example, by keeping data they hold both up to date and secure (files should be kept locked up, and computers should be passworded), by not disclosing personal information or transferring it outside the organisation, and by taking particular care when using laptops, etc, in other locations (password protection is essential, and personal information may not be shared; neither screens nor paper files should be left unattended at any time). All data kept must be accurate, current, fair, kept and disposed of safely. Misuse of personal data is a disciplinary offence, and may even constitute a criminal offence.

### References

As a general rule, references may only be given by either the General Manager or the Partnerships Manager at Voluntary Action – Leeds. However, other line managers may provide references for their own staff where appropriate, provided that these are checked and authorised, prior to sending, by either the General Manager or Partnerships Manager. Particular care must be taken when providing references, either employment-related or personal. Information relating to personal data (e.g. attendance records, discipline, etc) must not be provided without the express written consent of the data subject.

#### **b) External Data**

Voluntary Action – Leeds recognises its duty to safeguard the data it holds on external groups and individuals. To this end at regular intervals we conduct an audit of data held, dispose of outdated information, and arrange secure storage systems for current data including locked/passworded storage, and locked archive facilities. In addition, the following steps have been taken:

- All written materials (membership packs, payroll packs, forum membership packs, newsletter forms, training forms, generic

marketing leaflets, etc) have been designed to ensure that all data is being kept with permission.

- VA-L has ceased to supply mailing lists from its member lists unless the express consent of these members has been obtained first.
- Any VA-L member is entitled to know what data is kept on her/him, why, how it is kept, and who can access it. Any VA-L member may also see what data is kept on her/him and correct it if necessary; to do so, s/he should make a written request to the General Manager, who will contact her/him to arrange a mutually convenient appointment for this, and who will facilitate the occasion either in person or by ensuring the involvement of other relevant staff (e.g. Payroll).

### **Other Relevant Policies**

Various VA-L Policies relate to and should be read alongside this Policy – for example:

- (a) Statement of Written Employment Particulars
- (b) Guidelines on Confidentiality
- (c) Disciplinary Procedure
- (d) Staff Rules (part of Disciplinary Procedure)
- (e) Internet/Email Policy
- (f) Archiving Policy

Any questions or concerns about the implementation of this Policy should be addressed to line managers, and further information on data protection issues generally is available in the VA-L library or from [www.ico.gov.uk](http://www.ico.gov.uk)

*This Policy was formally adopted by the Trustee Board of Voluntary Action – Leeds on 20<sup>th</sup> June 2000; updated November 2006.*