The Trust for Developing Communities

Data Protection Policy

Policy number	16.0
Effective date	April 2013
Key contact	The Administrator
Number of pages	2
Review date	October 2015
Expiry date	April 2016

Introduction

This policy aims to ensure compliance with the Data Protection Act 1998, which refers to computerised and manual records of personal data.

1. Control of data collected and stored

Personal data collected by the Trust for Developing Communities (the Trust) shall be stored and processed fairly and lawfully, and only for the purposes for which it has been collected. It shall not exceed the purposes for which it is required. Specifically, personal data will be collected and stored to:

- process job applications
- maintain and process personnel and payroll records of employees
- maintain records of relevant personal details of staff, volunteers, members and trainees
- maintain personal details of clients using the services as required by staff (paid or unpaid) to carry out the service.

There is a tick box option included on the TDC application form which allows the applicant to agree to their form being filed so that TDC could contact them in the future if there were any suitable opportunities.

Otherwise, applications are to be stored for 12 months and then disposed of confidentially.

Special efforts will be made to ensure that sensitive data, such as that on health, ethnic origin, trade union membership etc. will not be kept in such a way that the subject's identity may be guessed, except where this is strictly necessary for personnel and payroll purposes.

2. Accuracy of data

All personal data stored by the Trust shall be accurate and kept up-to-date.
No personal data shall be stored longer than is necessary to provide services effectively.

3. Secure storage

All personal data held by the Trust shall be stored securely at all times. This means it shall be stored in offices accessible only to staff, and in locked cabinets accessible only to approved staff, namely:

- in the case of staff data, management, personnel and payroll staff
- in the case of client data, relevant team staff, and Trust management

All computerised data shall be protected by passwords so that it is accessible only to authorised staff as above. No personal data shall be removed from the Trust premises except for regular back-ups taken off site.

4. Access to personal data

Anyone on whom personal data is stored shall be informed of what information is stored and how it is processed, and of their rights to access their own records. They shall be given access to all information held on request free of charge at the earliest available opportunity, and permitted to have data corrected or erased if it is incorrect. Since changes to the EU data protection regulation in January 2012, users have the right to ask that data about them be deleted if there are no "legitimate grounds" for it to be kept.

5. Disclosure

No personal information shall be disclosed to another person or agency except with the express permission of the person concerned. The only exceptions to this relate to matters where the project is legally bound to pass on information, for example, in relation to Child Protection.