Telford and Wrekin
CVS
Involving, Inspiring, Supporting

Registered Office:
The Glebe Centre
Glebe Street
Wellington
Telford
Shropshire
TF1 1JP

Tel: 01952 567800
www.telfordandwrekincvs.org.uk

Data Protection & Confidentiality Policy

This policy supersedes any reference to data protection and confidentiality in the current Telford and Wrekin CVS Handbook.

PRINCIPLES

Data Protection Act 1984

The Data Protection Act was enacted on 12th July, 1984 and applies to personal data processed automatically (i.e. on computer) about living persons. The principle aim of the act is to ensure that individuals are protected from data, which is incorrect, unfair or disclosed illegally to another party. Under the Act it is an offence to make unauthorised disclosure, whether deliberately or through negligence, of information derived from data process by machine. The principles of the Data Protection Act are that personal data must be: -

- Obtained and processed fairly and lawfully.
- Held for the lawful purposes described in the data user's register entry.
- Used only for the purposes, and disclosed only to those people described in the data user's entry.
- Adequate, relevant and not excessive in relation to the purposes for which they are held.
- Accurate and, where necessary, kept up to date.
- Held no longer than is necessary for the registered purpose.
- Accessible to the individual concerned who, where appropriate, has the right to have information about themselves corrected or erased.
- Surrounded by proper security.

Data Protection Act 1998

The 1998 Data Protection Act is concerned with 'personal data'. The 'personal' part is relatively straightforward, referring to data about: -

- Identifiable
- Living
- Individuals

It therefore does not apply to information about companies or organisation, but it could apply to named contacts within those organisations. It does not apply to data, which is completely anonymous, but it does apply if you can identify people from the data combined

with other information held. It does not apply to historical information about people who have died, or to fictitious people.

'Data' is defined in the Act under four headings. For most purposes data essentially amounts to: -

- Information held on the computer.
- Information in relevant manual files.
- Information intended to become part of one of the above systems.
- Certain information held by the government and local government agencies to which the Data Subject has a right of access under other legislation.

The definition of data is wide, and the 1998 Act extends the definition in the 1984 Act in four main ways: -

- The 1984 Act excluded certain information held on computer; the 1998 Act makes no exceptions.
- The 1998 Act much more explicitly covers non-text data such as photographs, audio and video material, and biometric data (such as fingerprints, iris patterns or DNA samples).
- The 1984 Act did not cover paper systems, the 1998 Act does.
- The 1998 Act introduces a new category covering material intended to be put onto computer or to become part of a relevant manual system. 'Computer' is used here as shorthand for any equipment operating automatically.

Registration

Telford and Wrekin CVS is registered with the Information Commissioner as Data Controllers. All users of personal data, the data itself and its uses must be registered. It is not necessary for individual employees to register but it is important that the registration of Telford and Wrekin CVS is comprehensive.

Failure to notify any activities requiring registration to the Head of Finance and Resources and illegal disclosure of any personal data will be treated by the CVS as a breach of the Data Protection Act and will result in disciplinary action.

Under the Act individuals commit an offence if they knowingly or recklessly obtain or disclose personal data without the consent from the data controller. If a person has obtained data they are not entitled to, it is a further offence to sell it or offer to sell it. Any such offenses will result in disciplinary action.

It is important that all members of staff understand the need to prevent unauthorised disclosure of personal data and the need for data to be registered, accurate and secure.

Security

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of personal data, and against accidental loss or destruction of personal data. The following guidelines must be followed: -

- **Screen display –** Precautions should be taken to ensure that information displayed is not observed by unauthorised persons, in particular that display screen are not facing windows where the screen can be easily seen by passers-by or can be viewed by visitors. Computer displays should not be left unattended especially when personal information is displayed.
- **Printouts –** Printouts should not be left lying around. Unwanted printouts should be destroyed through the shredder.
- **Passwords –** Protect individual computers by using 'log-on' passwords. Ensure that your password is strong and secure by making it at least 8 characters long with a mix of numbers, capital letters and symbols.
- **Discs / memory sticks –** Keep in a locked drawer or holder when not in use.

Access Requests

Data subjects can ask to see all personal data you hold on them including manual files. The organisation has 40 days to comply with the request. You must provide the information that you held at the time when the Subject Access request was made. You must not tamper with the information to remove parts you would rather the Data Subject did not see, or do anything to the information that you would not have done in the normal course of events. Any access requests received should be directed to the Head of Finance and Resources.

Confidentiality

All information that:-

a) is or has been acquired by you during, or in the course of your employment, or has otherwise been acquired by you in confidence;
b) relates particularly to our business, or that of other persons or bodies with whom we have dealings of any sort and
c) has not been made public by, or with our authority;

shall be confidential and safe in the course of our business or as required by law you shall not at any time, whether before or after the termination of your employment with us, disclose such information to any person without our prior written consent.

You are to exercise reasonable care to keep safe all documentary or other material containing confidential information and shall at the time of termination of your employment with us, or at any other time upon demand, return to us any such material in your possession.