DATA PROTECTION POLICY

Employees may be required to give certain information relating to themselves in order that the Organisation may properly carry out its duties, rights and obligations as the employer. The Organisation will process and control such data principally for personnel, administrative and payroll purposes.

The term 'processing' may include the Organisation obtaining, recording or holding the information or data, or carrying out any set of operation or operations on the information or data, including organising, altering, retrieving, consulting, using, disclosing, or destroying the information or data. The Organisation will adopt appropriate technical and organizational measures to prevent the unauthorized or unlawful processing or disclosure of data.

Employees are requested to sign the attached consent form giving consent to the Organisation to process data relating to them which may include sensitive data.

In the course of your work you may come into contact with or use confidential information about employees, service users and stakeholders, for example their names, home addresses and medical information. The **Data Protection Act 1998** contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Mr. Leeford Smith, the Organisation's Service Manager. You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Organisation's disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The data protection principles

There are eight data protection principles that are central to the Act. The Organisation and all its employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

- race or ethnic origin
- political opinions and trade union membership
- religious or other beliefs
- physical or mental health condition

- sexual life

- criminal offences, both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

3. Adequate, relevant and not excessive. The Organisation will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is sound business reason requiring information to continue to be held.

4. Accurate and kept up-to-date. If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that the Organisation's records can be updated. The Organisation cannot be held responsible for any errors unless you have notified the Organisation of the relevant change.

5. Not kept for longer than is necessary. The Organisation will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Organisation decides it does not need to hold for a period of time will be destroyed after six months. Data relating to unsuccessful job applicants will only be retained for a period of six months.

6. Processed in accordance with the rights of employees under the Act.

7. Secure, technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff has access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on diskettes or other removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only authorised employees have access to that data. The Organisation has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

Your consent to personal information being held

The Organisation holds personal data about you and, by signing your contract of employment; you have consented to that data being processed by the Organisation. Agreement to the Organisation processing your personal data is a condition of your employment. The Organisation also holds limited sensitive personal data about its employees and, by signing your contract of employment, you give your explicit consent to the Organisation's holding and processing that data, for example sickness absence records, health needs and equal opportunities monitoring data.

Your right to access personal information

You have the right, on request, to receive a copy of the personal information that the Company holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You have the right on request:

- to be told by the Organisation whether and for what purpose personal data about you is being processed
- to be given a description of the data and the recipients to whom it may be disclosed
- to have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- to be informed of the logic involved in computerised decision-making.

Upon request, the Organisation will provide you with a statement regarding the personal data held about you. This will state all the types of personal data the Organisation holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Organisation reserves the right to charge you a fee of up to £10. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Service Manager.

If you wish to make a complaint that these rules are not being followed in respect of personal data the Organisation holds about you, you should raise the matter with the Service Manager. If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under the Organisation's grievance procedure.

Your obligations in relation to personal information

You should ensure you comply with the following guidelines at all times:

- do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this
- be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail
- if you receive a request for personal information about another employee or a service user, you should forward this to Mr. Leeford Smith who will be responsible for dealing with such requests
- ensure any personal data you hold is kept securely, either in a locked filing cabinet

or, if computerised, it is password protected

- compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, take this up with the Service Manager.

Please refer to details of the Data Protection Act 1998 (sections 7 and 8) in the Appendix for further information.

DISCLOSURES IN THE PUBLIC INTEREST

The **Public Interest Disclosure Act 1998** protects employees who raise legitimate concerns about specified matters. It makes provision about the kinds of disclosure which may be protected and the circumstances in which disclosures are protected. These rules are therefore intended to comply with the Act by encouraging employees to make disclosures about fraud, misconduct or wrongdoing to the Organisation, without fear of reprisal, so that problems can be identified, dealt with and resolved quickly.

Qualifying disclosures

Certain kinds of disclosure qualify for protection. These are disclosures of information which are made in good faith and which you reasonably believe tend to show one or more of the following matters is either happening now, took place in the past, or is likely to happen in the future:

- a criminal offence
- the breach of a legal obligation
- a miscarriage of justice
- a danger to the health or safety of any individual
- damage to the environment
- deliberate concealment of information tending to show any of the above.

Your belief must be reasonable, but it need not be correct. It might be discovered subsequently that you were, in fact, wrong, but you must be able to show that you held the belief and that it was a reasonable one to hold in the circumstances at the time. Note that it is not your responsibility to investigate the matter. That is the Organisation's responsibility.

The disclosure procedure

In order to qualify for protection, there are specified methods of disclosure, or procedures, which you must have followed in order to disclose one of the above matters. The Organisation encourages you to raise your concerns under this procedure in the first instance. If your concern relates to a breach of your own contract of employment, you should use the Organisation's grievance procedure. This procedure applies to all employees. In addition, agency workers and contractors who perform functions in relation to the

Organisation are encouraged to use it.

The procedure is as follows:

1. If you wish to make a qualifying disclosure, you should, in the first instance, speak to your line manager. Your line manager will endeavour to deal with your concerns as soon as possible and, in any case; within five working days from the time you make the disclosure. If it is not possible to respond within this time period, you will be given an explanation for the delay and be told when a response can be expected. In all cases, you will be informed of the outcome of the investigation and the Organisation's conclusions. If you do not wish to speak to your line manager because either you believe they are involved in the wrongdoing or for any other reason, you can instead speak to Mr. Leeford Smith or use the Organisation's Whistle Blowing Procedure. Disclosures should be made promptly so that investigation may proceed and any action taken expeditiously. Confidentiality will be maintained during the investigatory process to the extent that this is practical and appropriate in the circumstances. However, in order to effectively and thoroughly investigate a disclosure, the Organisation must be able to determine the scope of the investigation and the individuals who should be informed of the disclosure. The Organisation therefore reserves the right to involve other employees who may be better placed than the line manager to resolve the problem. Be aware that the investigation may involve you and other employees being asked to give a written statement.

2. Once the Organisation's conclusions have been finalised, any necessary action will be taken. This could include either reporting the matter to an appropriate external government department or regulatory agency and/or taking internal disciplinary action against relevant members of staff. If no action is to be taken, the reasons for this will be explained to you.

3. In the event that you feel the issue has not been satisfactorily resolved or you believe the investigation was inadequate, you may then raise the matter with The Service Manager of the Organisation. On receipt of such a request, the Service Manager will make arrangements to meet with you within five working days of the request being made. The Service Manager will then respond to the issue in writing within five working days of the meeting. If it is not possible to respond within this time period, you will be given an explanation for the delay and be told when a response can be expected. The Organisation reserves the right to arrange for another manager to review the case other than the manager with whom you raised the matter.

4. If, on conclusion of the above stages, you reasonably believe that appropriate action has still not been taken, you should then report the matter to the proper authority in good faith. The Act sets out a number of prescribed bodies or persons to which qualifying disclosures may be made. If in doubt about which matters have been prescribed to which bodies or persons, please speak to Mr. Mark Paffard, Sandwell Supporting People Team.

The Organisation always encourages employees to raise their concerns internally in the first instance, rather than externally.

General principles

- be aware of the importance of eliminating fraud or wrongdoing at work. Report anything that you become aware of that is illegal

- you will not be victimised, subjected to a detriment or dismissed for raising a legitimate matter under this procedure

- victimisation of an employee for raising a qualifying disclosure under this procedure will be a disciplinary offence and will be dealt with under the Organisation's disciplinary procedure.

Please also refer to the Organisation's Whistle Blowing Policy.
Please also visit www.opsi.gov.uk/acts/acts2000 for information on the Freedom of information Act 2000.