Data Protection Policy	**Date effective:** 20/06/12 **Approved by:** Board **Responsible for:** D of FCS **Review date:** FEB 16

1 About the Data Protection Policy

1.1 This policy applies to all employees and secondees. Consultants are obliged to adhere to this policy as part of their service agreement; contracting Managers are responsible for ensuring consultants' adherence.

1.2 The Director of Finance and Corporate Services is responsible for this policy. Please contact the Director of Finance and Corporate Services in the first instance for further information.

2 Policy

The organisation aims to fulfil its obligations under the Data Protection Act 1998 (DPA) to the fullest extent. The DPA sets out principles which should be followed by those who process data; it also gives rights to those whose data is being processed.

Therefore, the organisation endorses fully, and adheres to, the eight principles of data protection, as set out in the DPA (see FAQ section 8.2 below for further guidance on the eight principles).

Therefore, through appropriate management and diligent application of criteria and controls, the organisation will:

- observe fully the conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the DPA, i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards.

3 Designated Data Controller

3.1 As the organisation's 'designated data controller' the Director of Finance and Corporate Services will deal with all DPA matters.

Therefore, any member of staff, or other individual who considers that this Policy has not been followed in respect of personal data about them should raise the matter with the Director of Finance and Corporate Services. In addition, members of staff should seek guidance and advice from the Director of Finance and Corporate Services when dealing with DPA related issues and requests.

4 Staff Responsibilities

4.1 All members of staff are responsible for:

- checking that any information they provide to the organisation in connection with their employment is accurate and up to date
- informing the organisation of any changes to information they have provided, for example changes of address, either at the time of appointment or thereafter.

Members of staff should note that the organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

5 Data Security

5.1 All staff are responsible for ensuring that:

- any personal data they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, the information must be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

6 Subject Consent

6.1 In many cases, the organisation can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the DPA, express consent must be obtained.

Agreement to the organisation processing some specified classes of personal data are condition of employment for staff. This includes information about previous criminal convictions.

Therefore, the application forms that all prospective staff are required to complete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a form will prevent the application from being processed.

7 Access to Employee Data

7.1 The organisation aims to fulfil its obligations under the DPA to the fullest extent.

Procedure

Members of staff are allowed to have access to personal data about them held under the DPA which requires the organisation to respond to requests for access to personal data within 40 days. Details of an employee's personal data are; therefore, available upon request in accordance with the principles of the DPA.

The Data Protection Act 1998 gives data subjects the right to have access to their personal data at reasonable intervals. Should a member of staff request access to their personal data at any other time, the request must be addressed to the Director of Finance. The request will be judged in the light of the nature of the personal data and the frequency with which they are

updated. The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.

In the event of a disagreement between a member of staff and the organisation regarding personal data, the matter should be taken up under the organisation's formal grievance procedure.

Note: secondees would have to contact their employer for guidance where there is a disagreement relating to personal data.

Where staff members make additional requests for access to their personal data which are granted, a fee of £10 will be charged which must be paid to the Director of Finance and Corporate Services before a copy of the personal data will be given.

8 FAQ

8.1 *Question: What are the 'eight principles' of the DPA?*

Answer: In summary these state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for that purpose.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.