1. **Introduction**
   The Trust needs to keep certain personal data, for example about its staff and programme participants, to fulfill its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Trust complies with the Data Protection Principles which are set out in the Data Protection Act, 1998 and is registered with the Information Commissioners Office (ICO).

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

   The Trust and its entire staff who process or use personal information, particularly which which is pertinent to programme participants, must ensure that they follow these principles at all times. In order to ensure that this happens, the Trust has developed this Data Protection Policy.

3. **Status of the Policy**
   This policy has been approved by the Trust Management Committee, and any breach will be taken seriously and may result in more formal action.
Any member of staff or programme participant who considers that the policy has not been followed, in respect of personal data about themselves, should raise the matter with the General Manager.

4. Notification of Data Held & Processed
All staff, programme participants and other users are entitled to:

• Ask what information the Trust holds about them and why.
• Ask how to gain access to it.
• Be informed how to keep it up to date.
• Be informed what the Trust is doing to comply with its obligations under the 1998 Data Protection Act.

5. Responsibilities of Staff & Programme Participants
All staff and programme participants are responsible for:

• Checking that any personal data that they provide to the Trust is accurate and up to date.
• Informing the Trust of any changes to information, which they have provided, e.g. changes of address.
• Checking any information that the Trust may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, staff collect information about other people e.g. about programme participants’ course work or personal circumstances, or about members of staff in their department, they must comply with this Policy.

6. Data Security

• The Trust takes the protection of data and other private information very seriously. For current Client information it adopts a ‘user level’ approach to access the Trust’s Intranet server. This provides for three tiers………..‘read only’, ‘read and write’ and ‘admin’. These all require individual user names and passwords which, in turn, control the level of access and use.

• We aim to give Clients open internet access for job search sites, while restricting access to unsuitable sites, such as gambling. To achieve this we use the NAT System on our network, as well as a router firewall, to block unwanted sites and files from access.

• Thirdly, to archive all personal contact and other Client information, for long term storage, we use a PGP encryption programme to transfer the data onto a RAID NAS storage system. This is governed by a User Level Access System which prevents unauthorized access.
7. Rights to Access Information
Staff and programme participants have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. Any person who wishes to exercise this right should make the request in writing to the General Manager.

The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of request, unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

8. Publication of Information
Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information contained within externally circulated marketing material. Any individual who has good reason for wishing details in such material to remain confidential should contact the General Manager.

9. Subject Consent
The need to process data for normal purposes is communicated to all staff, and to programme participants at registration.