CONFIDENTIALITY

AND

DATA PROTECTION

POLICY

1. **Introduction**

i. Impel College Of London, needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. To comply with the law, information must be collected and used fairly, stored safety and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that 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.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorized access, accidental loss or destruction.

ii. The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed the Data Protection Policy.

2. **Status of the Policy**

i. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

ii. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

3. **Notification of Data Held and Processed**

i. All staff, students and other users are entitled to know:

- What information the College holds and processes about them and why.
- How to gains access to it.
- How to keep it up to date.
- What the College is doing to comply with its obligations under the 1998 Act.

4. **Responsibilities of Staff**

i. All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information, which they have provided. i.e. changes of address.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

5. **Data Security**

i. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

ii. Personal information should be;

- kept in a locked filing cabinet; or in a locked drawer; or
- if it is computerized, be password protected; or
- When kept or in transit on portable media the files they must be password protected.

iii. Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Department must be obtained, and all the security guidelines given in this document must still be followed.

iv. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist.
- Sensitive data is appropriately encrypted.
- Sensitive data is not copied onto portable storage devices without first consulting the Directors, in regard to appropriate encryption and protection measures.
- Electronic devices such as laptops or PDA's, and computer media (floppy disks, USB devices, CD-ROM's etc…) that contain sensitive data ARE not left unattended when offsite.

v. For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Director.

6. **Student obligations**

i. Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc are notified to the

Administrator.

7. **Processing Sensitive Information**

i. Sometimes it is necessary to process information about a persons health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognized that the processing of it may cause particular concern or distress to individuals, Staff and students will be asked to give express consent for the College to do this.

ii. The College will need to keep information about staff for longer periods of time, In general, all information will be kept for five years after a member of staff leaves the College. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

8. **Conclusion**

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution.