Code of Practice 1 - handling of personal data

1. Introduction

1.1 This Code of Practice, drawn up in association with the College's Data Protection Policy, relates to the collection, holding and disclosure of data relating to individuals. The Code provides best practice for staff and students of the College and other authorised persons who collect, process, disclose or have access to personal data in whatever medium that data is held. In the terms of the DPAct98 "processing" covers all aspects of handling personal data, including obtaining, recording, holding, retrieving, collating, disclosure, erasure and destruction of data.

2. Registration and Notification

2.1 The College has an obligation to notify the Data Protection Commissioner of collections of personal data held by its members and other authorised persons on computers or in relevant filing systems. If you hold or control personal data you must ensure that your use, or processing, of it is in accordance with the College's notification. You should inform the relevant Data Protection Coordinator (DPC) when a new dataset has been established or if the purpose for which personal data stored in a dataset, which has already been registered, has changed.

2.2 Any personal data held in networked datasets must be registered with the College Data Protection Officer by the CAU controlling the dataset through the relevant Data Protection Coordinator.

2.3 Anyone extracting personal data from a networked dataset to form their own dataset should register this new dataset, and the purpose for which it is being used, with their CAU's Data Protection Coordinator. Data Protection Co-ordinators will advise the College Data Protection Officer of it and s/he will decide if an amendment is required to the College's notification.

2.4 When applying to the College Data Protection Officer for registration or amendment to the College's notification, broad descriptions of the following are required:

- the classes of personal data held;
- the purposes for which it is used;
- the sources from which the data has been obtained;
- types of people to whom the data may be disclosed;
- those countries to which the data may be transferred.

2.5 The College's Data Protection notification is in the public domain and can be accessed via the website of the Information Commissioner's Office. It is also available for inspection, by arrangement, in the Central Secretariat. It should be noted that a register entry only shows what a data user is registered to do; it does not reveal whether the data user holds specific personal information on an individual.

3. Collecting and processing of personal data

3.1 Collection of Personal Data

3.1.1 Staff, and to some extent students, in CAUs collect both standard and sensitive personal data on employees, students and other individuals.
3.1.2 Most personal data which is collected on a day-to-day basis will be "standard", i.e. for general administrative purposes, and will cover categories such as:

- General personal details such as name, address, date of birth and next of kin;
- Details about class attendance, course-work marks and grades and associated comments;
- Notes of personal supervision, including matters about behaviour and discipline;
- Management of student clubs and societies.

3.1.3 Data Subjects must be informed of the purposes for which data are being collected at the point of collection. Any additional processing which is done in CAUs will necessitate the Data Subjects in those units being given the opportunity to opt out of such processing.

3.1.4 Some types of data are deemed to constitute sensitive data, a definition of which is given at Appendix 1, and such data, with a few exceptions, can be collected and processed only with the individual's explicit consent.

3.2 Processing all Standard Data

3.2.1 Data Users have a duty to make sure that they comply with the Data Protection Act and handle personal data in accordance with the data protection principles, which are set out in the College Data Protection Policy. 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 kept only for as long as is necessary for that purpose.
- Be processed in accordance with the Data Subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Be transferred to a country outside the European Economic Area, only where that country has equivalent levels of protection for personal data.

3.2.2 All personal data must be held securely and in confidence, subject to the disclosure provisions set out in this Code, and in accordance with the College's Information Systems Security Policy. All persons having access to such data shall treat as confidential all information about an individual (which is not otherwise in the public domain) which they may learn in the course of their work. They shall not communicate it to other persons or bodies except in accordance with this Code of Practice and the College's DP notification with the Information Commissioner.

3.2.3 Before processing any personal data, members of the College and other authorised individuals should study the checklist for recording data (Appendix 1).

3.2.4 Where any of the Data Protection principles are not followed data users may find themselves subject to College disciplinary procedures. If, in addition, a data subject suffers significant damage or
distress as a result, the individual Data User, as well as the management of the College, may be subject to investigation and liable to prosecution under the Act by the Data Protection Commissioner.

3.3 Processing Sensitive Data

3.3.1 The 1998 Act introduces a number of restrictions and conditions on data controllers who want to record and process this type of data, including an obligation to obtain the "explicit consent" of the relevant individual, before doing so.

3.3.2 CAOs will authorise certain individuals as the only persons in each CAU authorised to hold or process sensitive data.

3.3.3 The only exception to this will be if a non-authorised person member is satisfied that the processing of the data is necessary:

- in the best interests of the Data Subject, or the College; AND
- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances. In such instances, the non-authorised person must inform the authorised person of their action as soon as possible thereafter.

3.3.4 Authorised persons will be responsible for ensuring that all sensitive data is kept securely, whether held electronically or in a relevant manual filing system.

3.4 Disclosure of Personal Data to Third Parties

3.4.1 All disclosures of personal data must be consistent with the College's notification under the Data Protection Act which registers the purposes for which data is processed.

3.4.2 No data relating to a particular student, member of staff or other individual acquired in the course of an individual's duties should be disclosed to anyone (including other students or staff) unless:

- required for normal academic, administrative or pastoral purposes of College business, or
- the individual concerned has given permission, or
- they are required to do so in the discharge of regulatory functions or required by legislation, or
- in the case where, even though prior consent has not been given, disclosure is deemed to be needed to protect the vital interests of the Data Subject or it is required for the prevention or detection of crime or the apprehension or prosecution of offenders, or
- it is used for research purposes, where special conditions apply.

3.5 Transfer of Data Overseas

3.5.1 Posting personal data to the World Wide Web constitutes transfer of data worldwide. Subject to taking appropriate security measures, as set out in 3.6 below, personal data may be transferred to countries in the European Economic Area (EEA) without further restriction.

3.5.2 Personal data may be transferred to a country or territory outside the EEA only where:
• it is required for the performance of a contract between a Data Subject and a Data Controller, or
• for taking steps at the request of a Data Subject with a view to entering into such a contract, or
• where specific and informed consent of the Data Subject has been obtained for effecting such a transference, or
• where it has been established that the country/territory exercises a level of protection of that personal data sufficient to ensure the rights and freedoms of the Data Subject in the processing of that data.

3.5.3 Proper records must be kept justifying any decision made about such exempted transfers, or clear evidence can be demonstrated showing the Data Subject had given consent to the transfer, having been suitably informed.

3.5.4 In the absence of a sponsorship arrangement between the College and an external body in respect of a particular student, personal data should not be disclosed in response to a request from non-EEA governments, agencies or organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without specific informed consent of the Data Subject(s) concerned, nor should such data be disclosed to such bodies for the purposes of determining liability to attend National Service without such consent.

3.6 Security

3.6.1 Proper security measures must be applied to all methods of holding or displaying personal data and appropriate measures taken to prevent loss, destruction or corruption of data. For fuller details on security measures see the College Information Systems Security Policies, associated Codes of Practice and Guidelines on the College website.

3.6.2 Staff, students and authorised third parties are not permitted to remove from the College personal data with the intention of processing this information elsewhere, unless such use is authorised by the Data Owner and that authorisation recorded. Removing data in this way must not compromise the standards of security operating within the College, and the Data Protection Principles should be observed at all times. This includes the storage and processing of data on external Personal Storage Sites e.g. iSpace or Hotdrive.com

3.7 Subject Consent to Processing

3.7.1 Agreement to the College processing some specified classes of personal data for normal College administrative purposes is a condition of acceptance of a student on to any course, and a condition of employment for staff. Therefore, all prospective staff and students will be asked to sign a Consent to Process form regarding particular types of information when an offer of employment or offer of a course place is made. A refusal to sign such a form could result in the offer being withdrawn.
Appendix 1 - checklist for recording and retention of personal data

1. Do you really need to record the information?
2. Is the information "standard" or is it "sensitive"?
   a. If it is sensitive, do you have the Data Subject's express consent?
3. If you do not have the Data Subject's express consent to process, are you satisfied that it is in the best interests of the Data Subject to collect and retain the sensitive data?
4. Has the data subject been told how the data will be processed?
5. Are you authorised to collect/store/process the data?
6. If yes, have you checked that the data are accurate?
7. Is it clear who else has a right to access/process these data?
8. Do you have mechanisms in place to ensure that the data are kept securely whether held electronically or in a relevant filing system?
9. Are you clear as to how long you may retain these data?
10. Do you have procedures in place to ensure that the data are kept up to date?
11. Do you have procedures in place to remove these data securely when it is no longer needed?
12. Do you have procedures in place to remove these data where a data subject exercises their right for it not to be processed;

[1] A collection is normally a dataset of information held electronically or information in a relevant filing system as defined in the Data Protection Act 1998. It is identified by a broad description of the data, and what the user intends to do with it, rather than any specific detail.

[2] Each Department/Division/Centre, Academic Service, College Central Administration Division, the Imperial College Union and each wholly-owned College Company, known as College Administrative Units (CAUs) has a Data Protection Co-ordinator