Data Protection Policy

Background
The 1998 Data Protection Act first came into effect in March 2000, and was extended to cover structured manual records in October 2001. Underlying the Act is a set of principles governing good practice; the College is also required to notify its use of personal data to the Information Commissioner, and information on the categories of data held are on the Commissioner’s web site.

The Council of the College adopted this Data Protection Policy on 4 July 2002. Guidance Notes for the information of both staff and students are also attached.

Data Protection Policy
- Introduction
- Data Protection Principles
- Rights of staff and students
- Responsibilities of staff and students
- Responsibilities of those processing data
- Data Security
- Rights of Access to information
- Archiving of information
- Data Protection Officer

Data Protection Guidelines
- College Registration
- Guidelines for Staff
- Security
- Use of personal data in research
- Holding and release of assessment information
- References
- Checklist for those recording data

Introduction
The College needs to keep certain personal data about its students and staff to fulfil its objectives and to meet its legal obligations to funding bodies and Government. Certain research projects, particularly in the School of Medicine & Dentistry, also need to record personal data for research and analysis. To comply with the law, all information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles in the Data Protection Act. This policy applies to personal data held on every computer owned, or operated by the College. It also covers personal data held in paper-based manual filing systems anywhere in the College that has been collected for College purposes.

Data Protection Principles
The eight data protection principles in the Data Protection Act are 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 those purposes.
[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 secure 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.
Rights of staff and students
All staff and students on whom the College, or any part of the College (for example, a department) holds personal information are entitled to

• ask what information is held about them and why;
• gain access to it;
• be informed how to keep it up to date.

‘Access’ involves access to the data on a ‘read only’ basis; it does not include the right to amend or update data, although any individual has the right to draw attention to any errors and request they be corrected.

Responsibilities of Staff and Students
All staff and students are responsible for

• checking that any personal data that they provide is accurate and up to date;
• notifying the College or department of any changes to the information that they have provided, such as changes of address;
• checking any details of information that the College or department holds, and may send to them from time to time for validation purposes.

Responsibilities of those processing data
If, as part of their responsibilities, staff collect information about other people, they must comply with this Policy and the related Guidelines.

Where data is regarded as ‘sensitive’, express consent must be obtained from the data subjects (ie, the persons to whom the data relates) to process the data. Sensitive data is defined in the Act as that relating to ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of criminal offences, or criminal convictions.

Data Security
Data must be kept securely, which means that precautions need to be taken against physical loss or damage, and that both access and disclosure must be restricted. Staff and students are responsible for ensuring that:

• all personal data is kept securely;
• personal information is not disclosed, by any means (orally, in writing or otherwise) to any unauthorised third party.

Detailed advice on data security appears in the Guidelines.

Right of access to information
Staff, students and other users of the College have the right of access to any personal data about them that is held on computer and in paper-based manual filing systems (see above for the definition of ‘access’). Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer. There will be a minimum charge of £10 for each request: if the costs of providing the data subject with access to his/her data exceeds this, the full charge will be made. The College is obliged to respond to a request within 40 days, but will normally respond within 14 days unless the request is complicated or involves access to archived records.

Archiving of information
The College is in the process of developing a formal policy on the retention of staff and student data, which responds to the data protection principle that information must be kept no longer than is necessary.

Data Protection Officer
The Data Protection Officer is the Academic Registrar, Dr Peter Holiday. He can be contacted in Room E12 of the Queens’ Building, telephone [13] 5072 or by e-mail on p.g.holiday@qmul.ac.uk.
Data Protection Guidelines

The Guidelines expand on the College's Data Protection Policy, and present best practice for the guidance of staff involved in handling personal data.

College Registration
Under the 1998 Act, the College is required to have a single registration (now called 'notification'); the reference is Z5507327. Details of the current registration can be accessed on the Information Commissioner's web site at http://www.dataprotection.gov.uk/.

The registration has been prepared to cover all the activities and types of data likely to be processed by a large, multi-faculty research based institution. But it is essential that, if a new research project is being set up involving the use of personal data, the person responsible contacts the Data Protection Officer with details, so that he can satisfy himself that the existing registration is adequate and, if not, to arrange for the registration to be updated.

Important Note – these Guidelines refer to 'processing' data. The Act gives a very wide interpretation to the word 'processing': it covers collecting data; holding data; sorting data; destroying data, etc. Every person who holds any personal data about another individual in a file that enables that data to be retrieved is 'processing data'.

Guidelines for staff
1 All staff process data about students on a regular basis – for example, when marking coursework and examinations, writing reports or references, or as part of their academic advisory role. The College notifies students, in the Students Guide, that it undertakes this kind of processing (as it is required to do). The kind of information that staff deal with on a day to day basis is described in the Act as 'standard' information, covering such things as:
   • general personal details e.g. name and address;
   • details about attendance, coursework marks and grades and associated comments;
   • notes associated with personal supervision, such as choice of course units.

2 Information about a student's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is 'sensitive' data and should generally only be collected and processed with the student's specific consent. Only a few staff will ever need to process this kind of information. These staff must be made aware of the special restrictions on the data that they hold. If staff need to record sensitive information – for example, for health reasons prior to taking students on a field trip – they must contact the Data Protection Officer well in advance to ensure that the requirements of the Act will be met.

3 Staff may also collect and process data about other staff in the College. Heads of Departments will almost certainly process data about the staff in their departments. The Personnel Office regularly circulates members of staff with the information held on them, both to inform them of the categories of data that are held, and to check its validity. Most of this information will be standard data, but if, for any reason, sensitive data has to be processed, then the Director of Human Resources will seek the express consent of the individuals concerned.

4 All staff have a duty to make sure that they comply with the data protection principles listed in the Data Protection Policy. In particular, staff must ensure that records are:
   • accurate;
   • up-to-date;
   • kept and disposed of safely;
   • processed in accordance with the data subjects’ rights.

5 Staff must not disclose personal data to any unauthorised third party. It will usually be obvious which individuals are ‘authorised’: for example, students’ marks must be disclosed to the department’s examinations officer so that they can be processed. As a general rule of thumb, the College will have
procedures covering the permissible processing of data; any processing outside those procedures should be questioned. The only exception will be if the disclosure is necessary in the case of a medical emergency: the Data Protection Officer should be informed before any action is taken, or as soon as possible thereafter.

6 Any information on the College’s external web is in effect the world-wide publication of that data; personal details should accordingly not appear on the web without the explicit permission of the individual(s) concerned.

7 The Data Protection Officer also has authority to agree to the release of personal data to the police when they are in pursuit of an active investigation, but this will only be done in person to an officer after the production of identification.

Data Security
8 The requirement to keep data securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff should ensure 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 unauthorised third party.

9 All personal information in the form of manual records should be kept in a locked filing cabinet or in a locked drawer. If the information is computerised, it should be password protected, with passwords being regularly changed, so that only authorised people can view or alter confidential data; or kept only on a disk which is itself kept securely in a desk or cabinet to avoid physical loss or damage. Laptop computers and PDAs are not considered secure, and therefore personal data should not be stored on laptops or PDAs.

10 To avoid unauthorised disclosure, care must be taken to site PCs and terminals so that they are not visible except to authorised people. Screens should not be left unattended when personal data is being processed. Similarly, care must be taken to ensure that manual records, e.g. staff or student files, or printouts containing personal data, are not left where they can be accessed by unauthorised staff.

11 When manual records, or printouts containing personal data, are no longer required, they should be shredded or bagged to be disposed of securely. Staff will need to keep sufficient information to be able to provide references, which could be required some considerable time in the future.

12 Particular care must be taken of any data taken away from the College, for example manual records to be used at home, or computerised data for use on portable computers or home machines. Students should not take patient data away from the College without express permission. Ensure that all work is kept confidential and, in the case of computerised information, that files are not exposed to risk from virus infection.

Use of Personal Data in Research
13 There are some exemptions from the 1998 Act for personal data processed for academic, scientific, historical or statistical research. Provided that the personal data has been obtained fairly and lawfully, the subsequent use of that data for research purposes will not breach the second data protection principle. Data collected for one piece of research can be used for other research, and may be kept indefinitely. However, there must be no direct consequences for any of the individuals in respect of whom the research is carried out and the personal data must not be processed in a way which is likely to cause damage or distress to any individual.

14 In order to avoid subject access provisions, the results of research or statistics should not be made available in a form that identifies the individuals concerned. Wherever possible, researchers should follow a principle of ‘pseudonymity’ in handling personal data and, for example, avoid the storage of names and addresses directly on computer by relying on reference codes instead.
When researchers wish to collect personal data for medical research, the Research Ethics Committee will ask for confirmation that the data will be collected in accordance with the Data Protection Act. The College procedure requires that the responsible researcher contacts the Data Protection Officer, and provides him with:

- a brief outline of the research project;
- a summary of the personal data to be collected;
- how the data will be collected, and what information will be given to the data subjects;
- how the data will be processed
- how the data will be stored and eventually disposed of.

The Data Protection Officer will then check to confirm that the project is covered by the College’s registration and, if necessary, arrange for the registration to be amended.

College policy is that, when a research project has been completed, the original data should be destroyed in a secure manner unless the relevant research protocols require that it be retained for reference in the event of a subsequent query. Data should not be retained in the event that it may, in the future, be of use in another project, as it is not possible to ensure that the objectives of any such future project will conform to the conditions under which the data was originally collected.

**Holding and release of assessment information**

The Data Protection Act allows an institution to withhold provisional assessment marks that are being processed to produce a final marks schedule, although there is a time limit within which this processing must be complete. As the College has already approved the release of the marks for individual elements of a unit, this will cause no problem. The marks for individual items of assessment should be retained until at least 3 months after the meeting of the examination board that validates the marks in the event of any requests for review of the results.

Examination scripts are not subject to access, but it has been argued that the comments made by individual examiners could be. Some institutions have therefore decided to ask markers to write their comments on a separate sheet that can be given to data subjects; others arrange to transcribe the comments in response to requests for disclosure. A solution used by some departments is for markers to make their comments on a separate sheet, which is retained until the marks are finalised at the examination board, and then destroyed. If the destruction of the comments is part of the standard procedure for processing the marks, this is acceptable.

It is not clear whether the Minutes of examination boards are subject to access, although one or two recent statements suggest that they may be. In any case, it is sensible for examination board secretaries to ensure that Minutes are purely factual.

**References**

Care should be taken when writing confidential references, whether these are for staff or students, or for external or internal (eg, promotion) purposes. A confidential reference given by the College to a third party, for the purposes of education, employment, training, etc should remain confidential and is exempt from the subject access provisions, in that the subject of the reference cannot gain access to the reference from its author. A received reference may also be withheld. However, institutions are increasingly operating on the assumption that references will shortly be accessible to the subject of the reference.

The writers of reports and references, whether relating to students or to staff, are therefore advised to concentrate their comments on factual matters (eg, dates of attendance; course-units passed, duties performed); any subjective observations or academic judgements must be based on, and substantiated by recorded factual data. Avoid comments on an individual’s personal life.

The author of a reference has a duty at law to be fair to both the subject of the reference, and the individual or institution to whom the reference is directed. Therefore, if a student’s record includes significant information to his/her detriment, it would be advisable to consult the Data Protection Officer on how to address this issue.
Checklist for those recording data

23 It is important to consider the following questions:

• is this information really needed?
• is the information ‘standard’ or ‘sensitive’?
• if it is sensitive, has the data subject's express consent been obtained?
• has the subject been informed that this type of data will be processed?
• has authority to collect/store/process the data been obtained?
• has the accuracy of the data been checked with the data subject?
• Will the data will be securely held?
• if the consent of the data subject to process the data has not been obtained, is it clearly in the best interests of the student or staff member for the data to be collected/retained?
• For how long will the data be kept, and are there arrangements for its secure disposal?

24 Further information and advice can be obtained from the College’s Data Protection Officer, Dr Peter Holiday, Academic Registrar, e-mail p.g.holiday@qmul.ac.uk.

Approved by Council
July 2002