

Guidance Notes for Staff on Handling Students' Personal Data

Introduction

1. These notes are for staff whose duties include the handling of students' personal data (held both in paper files and electronically). They provide practical advice for the maintenance of student files, how to handle enquiries for information about students and how to deal with issues relating to the release of students' personal data. See, in particular:
 - Student Files (paras 9 - 12)
 - Parents (para 16)
 - Sponsors (para 18)
 - Press (para 19)
 - Police (para 20)
 - Access to a student's own records (para 26)
 - References (para 28)
2. The Data Protection Act 1998 came into force on 1 March 2000. This Act implements a European Data Protection Directive which sets a standard for data protection throughout all the countries in the European Union. The new Act reinforces existing good practice (set in place under the previous Act, 1984), extends the rights of individuals and increases the responsibilities of data controllers. The Act has implications for the College in relation to the collection and use of a vast amount of personal data every year – staff records, names and addresses of those requesting course information, application and student details, examination marks, residence information, references, fee collection and many other administrative matters.
3. These notes should be read in conjunction with the College's Data Protection policy, which was approved by the Council on 4 July 2002, and is available on the web site at

<http://www.rhul.ac.uk/FOI/dataprotectionpolicy.html>

Definitions

4. 'Students' Personal data' means almost all information about, or correspondence identifying or relating to, an identifiable student. These notes also apply to applicants for admission to the College and to former students. Personal data includes names, addresses, nationality/domicile, sponsorship details and assessment results, as well as more obviously 'sensitive' information. The Data Protection Act applies to all of this record-keeping – and it is especially strict about the handling of the more sensitive types of data. Data which is *sensitive* must be treated more carefully in terms of deciding whether it is necessary to obtain it from the student, how to obtain it, whether it is permitted to disclose it to third parties and its storage.

5. The Data Protection Act 1998 identifies sensitive personal data as including data on ethnic origin, social class, physical and mental health (including, for example, how many days' sick leave an individual has had), sex life, religion or beliefs, political opinions and information relating to alleged or actual criminal offences.
6. The medium in which the data is held does not matter. The same guidance applies whether the information is held on paper, computer/magnetic media, microfilm, or in any other way – so a typical student file comes under these guidelines. In fact, any data held in a 'relevant filing system' is now subject to UK Data Protection legislation. A 'relevant filing system' is one in which the information is held in a structured way, for example by name or HEMIS number, and from which it is easy to retrieve information relating to a given individual. Such files will usually exist in the Registry, in academic departments, and in many cases in other departments such as Finance or the Dean of Students' Office.

The Processing of Students' Personal Data

7. There are statements in the Student Handbook (published annually), and on registration and enrolment forms, setting out for students the purposes for which data is collected, and indicating how they may deal with any data protection queries. The College must comply with data protection legislation by taking steps to ensure that personal data that is collected and processed must be for specified, explicit and legal purposes, and the data held must be accurate, relevant and not excessive to those purposes. There are obligations on the College to ensure that student personal data is kept secure, up-to-date and for no longer than necessary.
8. The College is required to collect and provide information on every student to certain external agencies. These bodies include the Higher Education Statistics Agency, local education authorities and other grant-awarding bodies, the Student Loans Company and taxation authorities. The College is also obliged to release information to the Police and similar law enforcers as part of criminal investigations, and in some instances, to officers of the Court in relation to civil proceedings. In certain circumstances, relating to the recovery of outstanding debt, data may be passed to debt collection agencies acting as the College's agents (see para 21 below).

Student Files

9. Wherever possible, the contents of a student's file should be limited to documents which reflect normal College business, and which have either already been copied to the individual in question, or could be so copied without any problem. Retaining documents which contain comments or judgements on individuals which are of a negative nature and unsupported by evidence should be avoided. You should seek to minimise instances where the file contains documents which you would be unhappy or embarrassed to have to show to the student(s) to whom they relate. If you find yourself in the uncomfortable situation of being asked to file documents which you feel contain negative and unsupported judgements on individuals, you should raise such cases with your line manager, or (if this does not resolve the situation), directly to the College's Data Protection Officer (see para 30 below).

10. There may well be circumstances in which you create 'private' files on students, separate from the main departmental file. The case for doing so has to be justified as being in the interest of that individual, e.g. where the data are particularly sensitive, but bear in mind that the individual almost certainly still has a right of access to that data under data protection legislation. Students will almost invariably be entitled to see any internal references or appraisals. In general, where you are in doubt about the best way to proceed, seek advice from the Data Protection Officer. Advice relating to files that are developed to deal with disciplinary cases, or that arise from complaints or appeals, is given in para 27 below.
11. If you can see opportunities for reducing paper filing (e.g. by relying on the central student database or paper records) and/or unnecessary duplication or fragmentation of files on students in your area, then please take action. Not only will this reduce duplication of filing effort (and duplication of judgement about difficult cases), but it will also help the Data Protection Officer if he needs urgently to pull together all of the documents held about an individual, in response to a subject access request. You should be aware that the College retains student records indefinitely; seven years after the student leaves the College such records are currently transferred to a CD-ROM format.
12. The contents of student files are confidential to any third party, and should not normally be shown to the student in question without that student having made a formal application to the Data Protection Officer. So, wherever feasible, student files should be transferred by hand, rather than via the internal post, and a student should never be asked to take his/her own file (or, any other student's file) to another office unsupervised.

Internal Enquiries About Student Data

13. You may release student personal data to other College staff who require that information in order to carry out their normal duties. This may be done electronically or using paper. Note that this does not include the non-College organisations on the campus (e.g. the bookshop or the bank). You should exercise care in dealing with such requests. It would not be appropriate, for instance, to release a student's home address or telephone number to a colleague without good reason.
14. In most cases it is likely that the enquirer will be well-known to you, and you will not be in any doubt about her/his identity. However, there will be some occasions where you are contacted by an unfamiliar staff member and you are not certain that the person is entitled to the data. Where you receive such an enquiry by telephone, it is recommended practice to call the enquirer back on a verifiable telephone number. For unfamiliar in-person enquirers, you should ask for some identification.

External Enquiries About Student Data

15. You should not disclose personal data about students or former students to anyone outside the College without the written consent of the person concerned, or as otherwise set out in the above Notes. Data may be disclosed in the following circumstances:
- (i) in the completion of statutory returns, for example the Higher Education Statistics Agency or the Student Loans Company, by staff whose job it is to make such returns;
 - (ii) to the University of London, where there is a valid business reason for doing so, for example to the Warden of a University Hall of Residence or the University Careers Service;
 - (iii) to the Police in the course of an investigation into a serious criminal offence, or in response to a search warrant (the College Secretary should be informed in all such cases), see para 20 below;
 - (iv) to UCAS and other admissions agencies, in relation to the admissions process, by staff whose job it is to liaise with such bodies;
 - (v) with the agreement of the Principal, a Vice-Principal, the College Secretary, the Head of Personnel or the Dean of Students, as appropriate, if there is a demonstrable emergency or risk to life.
16. Students' relatives or spouses do not have any general right to information about their child/partner/relative (which they often assume). Enquiries of this sort are often difficult to handle without losing the goodwill of the enquirer. It is good practice to offer to pass on a message. If there are difficulties that you cannot resolve you should refer to your line manager or the Data Protection Officer. A Code of Practice in relation to Parental Contact can be seen on the web site at:
- <http://www.rhul.ac.uk/For-Staff/Codes-of-practice/Parental-contact.pdf>
17. Other students do not have any special rights to information about their fellow students. Again, it is good practice, if practicable, to offer to pass on messages (and students will be able to send e-mails to their fellow students), but personal data should not be disclosed, other than as set out in para 15, above.
18. Sponsors and similar bodies (LEAs, Embassies, High Commissions, private companies, charities, etc) do not have a general right to access 'their' students' personal data (although in some cases, the College may undertake routinely to provide academically-related information, such as progress reports, to sponsors. Such arrangements should be documented, so that it is clear that the student is aware of, and has consented to, them). Parents may feel that because they contribute to the cost of their children's courses, they are sponsors, but this paragraph does not apply to parents.

19. Enquiries from media organisations concerning named individuals or other enquiries relating to students should always be referred to the Press and Public Relations Officer – Katie Price – ext 3967.
20. The College has an obligation to give reasonable assistance to the enquiries of law officers in connection with their investigations. Law officer enquiries should, if at all possible, be referred to the Head of Registry or the College Secretary, as should enquiries from other government agencies (e.g. HM Customs). If this is not possible, having established the bona fides of the law officer (which might include obtaining written confirmation of authority to act and the reason for acting), the person handling the enquiry may release the data directly, having followed this guidance:
 - (i) If the enquirer is a Court Bailiff, you must *insist* on referring him/her to the College Secretary. These enquiries are not usually urgent (although they may be presented as such) but must be dealt with consistently.
 - (ii) If the enquirer is a Police Officer whose identity you have confirmed, and there are urgent reasons for releasing the data (i.e. the student has become a danger to self or others, or has committed / is about to commit a crime) then you may release the information.
 - (iii) Take a note of all the details (the student in question, the Police Officer's identity, the information requested, the reason given, and exactly what information was provided) and copy this (marked 'confidential') to the College Secretary.
 - (iv) Enquiries from Authorised Officers of the Department for Work and Pensions, in connection with enquiries being conducted under the Social Security Fraud Act 2001, should be referred to the Head of Registry, who is the main point of contact for such matters.

Provision of Data to External Agencies

21. The College may, from time to time, enter into agreements with external agencies that require the release of students' personal data, eg for surveys, mailings or the collection of debts. In these circumstances, it is important that there is a clear, written agreement with the external agency concerned, which sets out the data to be used and the arrangements for its secure storage and eventual destruction. The external body in such cases is acting as an agent of the College. The students affected should also be notified, well in advance, of what is being done and given an opportunity to query the process.

The Columbus System

22. The CO LUMBUS s ystem will enabl e members of sta ff to a ccess the following student data:
- Name
 - Date of birth
 - Home address
 - Local address
 - Home telephone number
 - Local telephone number
 - HEMIS, HESA and SLC number
 - Reason for leaving
 - Fee status information
 - Course details
 - Assessment/Results information
23. Access to this data will be restricted to me mbers of sta ff who ha ve c omputer user names and passwords, and who h ave a business reason for access. Access will be administered through the Registry. This data must be treated in accordance with these Notes.

Access by Students to their Own Records

24. Under the 1998 D ata Protection A ct students have the ri ght to see most data, including e-mails, held about them. All persons about whom pe rsonal data are held (hereafter known as “data subjects”) are entitled to:
- know what information the College holds and processes about them and why;
 - know how to gain access to it, and where appropriate, to have such data corrected or erased;
 - know how to keep it up to date.
25. Under the terms of the Act, individuals are entitled to see any data about themselves only if it is stor ed in a structured filing s ystem from which they can be identified. There are some exceptions to subject access, for ex ample, where confidentiality to a third party would be compromised and outweighs the rights of the person making the request.
26. Students who ask for ac ccess to pe rsonal data should be referred to the College Secretary, Founder’s East Room 32. It will be his duty to establish the identity of the enquirer, to initiate a r equest for th e relevant data and to ensure th at such data are provided within the period of 40 days specified in the Act. A fee of £10 (as permitted under the Act) will be cha rged for each request. In order to en able the College to respond promptly and appropriately, enquir ers will usuall y be asked to indicate the nature of the personal data that they require and its location. (A separate note will be published about examination results.)

Disciplinary Cases, Appeals and Complaints

27. Considerable amounts of personal data will be generated and filed during disciplinary investigations, appeals against decisions of examination boards, complaints and similar cases. Members of hearing committees or panels may well keep private files as they are given documents to read and assess. As soon as the process has been concluded, all such "private" files should be returned to the officer servicing the process. That officer should retain one full set of papers and, unless given other instructions by the Chair of the Investigating Committee, destroy all others, using the confidential waste disposal system, until three years after the conclusion of the case, when that set of papers should be destroyed, other than a summary of the outcome, which should be placed on the student's personal file in the Registry.

References

28. Guidance on the provision of references for students was circulated to Heads of Departments and others in June 2001. It can be seen on the web site at:
- <http://www.rhul.ac.uk/Restricted/Codes/references-guidance-note.pdf>
29. Confidential references given or to be given by the College for the purposes of education, training or employment are exempt from the subject access provisions of the Data Protection Act. This exemption is not available for confidential references **received** by the College (i.e. a student will be entitled to see a reference received by the College, even if marked "confidential"). Should a student make such a request, it should be referred to the Data Protection Officer; see para 30 below.

Further Information

30. Further information or guidance may be obtained from:
- the College's data protection policy (see para 3 above)
 - the College's Data Protection Officer – Mike Miller, College Secretary – Founder's East Room 32 (tel: 01784 443550, fax: 01784 433619, e-mail m.miller@rhul.ac.uk).

M A Miller
College Secretary
14 August 2002