Chapter 15 University employment of its students: security aspects

Introduction

The University is increasingly employing its own students in a wide variety of areas. This development is to be encouraged. However students should be aware that there are security implications which may limit the availability of certain types of employment. The principles set out below describe these limitations and are intended to protect DMU students in employment with the University.

1 Principles

1.1 No student should by virtue of University employment have access to sensitive data. This includes:

- personal data concerning individuals, whether staff, applicants or students of the University;
- data of commercial sensitivity to the University.

1.2 No student should have access to areas of the University where sensitive data are kept. This includes faculty and departmental offices, Student and Academic Services, People & Organisational Development and Finance.

1.3 No student should be employed in activities which are sensitive. These include, but are not limited to:

- examination administration,
- registration and student records,
- admissions records administration,
- issuing results notifications,
- invoicing,
- cashiers' activities,
- debt chasing.

This does not preclude the employment of students in recruitment or admissions activities, acting as advisors, guides student ambassadors or 'runners'. Students can also be employed in catering, library, estates and technical work.

2 Employing department's responsibility

2.1 It is the responsibility of the employing department to assess the level of risk involved in employing students in their area. Some data are less sensitive than others. For example, it may be appropriate, under controlled circumstances, for a student to have access to names, addresses and final results of current or former students; but it would not be appropriate for students to have access to the grades of other students, nor to have rights of amending any data.

Where students are employed in areas of the University where there is potentially indirect access to sensitive information the employing department must adopt procedures and measures which minimise risk. For example, adoption of a clear desk policy with confidential information kept locked.

2.2 If a potential employer of students is in any doubt s/he should check the matter with the appropriate data owner and with the Director of People & Organisational Development. These have the right of veto. Data owners are:

Student data: Director of Student & Academic Services
Finance data: Director of Finance
Personnel data: Director of People & Organisational Development.

2.3 A potential employer should note that a student registered on a full-time De Montfort University programme should not undertake paid employment in excess of 15 hours per week as this cannot be consistent with the health and well being of the student or with satisfactory completion of their programme (see Chapter 1, paragraph 3.9).