

DATA PROTECTION POLICY

1. Introduction

1.1 The College needs to keep certain information about its employees, students and other clients/relevant bodies to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and Government met. To comply with the law, 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 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 not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than 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
- not be transferred to a country outside the European Economic Area, unless that country has adequate levels of protection for personal data

1.2 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 this Data Protection Policy.

2. Status of the Policy

2.1 It is a condition of employment that employees abide by the rules and policies made by the College from time to time. Any failures to follow this Policy may, therefore, result in disciplinary proceedings being invoked.

2.2 Any member of staff who considers that the Policy has not been followed in respect of personal data about him or herself, should raise the matter with the Compliance Officer/College Secretary initially. If the matter is not resolved it should then be raised in accordance with formal grievance procedures.

3. Notification of Data Held and Processed

3.1 All staff, students and other clients/relevant bodies are entitled to:

- know (on payment of a fee, which shall not exceed £10.00) what information the College holds and processes about them and why
- know how to gain access to it
- know how to keep it up to date
- know what the College is doing to comply with its obligations under the 1998 Act (although this is not an absolute entitlement)

The College will therefore undertake to provide all staff and students and other relevant users with a standard 'information statement'. This will state all the types of data the College holds and processes about them, and the reasons for which data is processed. The College will endeavour to do this at least once every three years, or earlier, when notification of a change in data is made.

4. Responsibilities of Staff

4.1 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)
- checking the information that the College will send out from time to time, giving details of information kept and processed about staff
- informing the College of any errors or changes.

4.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about student course work, staff development reviews, references to other academic institutions, or details of personal circumstance), they must comply with the provisions of the Act. Appropriate training will be provided for staff, from time to time.

5. Data Security

5.1 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 unauthorised third party

5.2 Staff should note that unauthorised disclosure will usually be regarded as a disciplinary matter, and may be considered a matter of gross misconduct in certain instances.

Personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on disk which is itself held securely

6. Student Obligations

- 6.1** 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 student registration office as appropriate.
- 6.2** Students who use the College's computer facilities may, from time to time, process personal data. If they do so, they must notify the Compliance Officer. Any student who requires further clarification about this should contact the Computing Services Manager.

7. Rights to Access Information

- 7.1** Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should apply in writing to the Executive Officer (Administration) in respect of staff, or the Registry Manager in respect of students.
- 7.2** The College will make a charge of £10.00 on each occasion that access is requested.
- 7.3** The College aims to comply with requests to access personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained, in writing, to the data subject making the request.

8. Publication of College Information

- 8.1** It is the College's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:
- names of College Governors
 - list of staff/profiles
 - College Regulations and Management Guidance Notes
 - list of achievements of staff/students
- 8.2** The College's internal telephone directory will not be a public document but will be accessible via the Intranet.

8.3 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Controller (College Secretary).

9. Subject Consent

9.1 In many cases, the College only processes personal data with the consent of the individual. In some cases, if the data is sensitive (as defined by the 1998 Act), **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

9.2 Certain staff may come into contact with young people between the ages of 16 and 18. The College has a duty under the Children's Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

9.3 The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will also use the information in the protection of the health and safety of an individual, and will need consent to process in the event of a medical emergency, for example.

10. Processing Sensitive Information

10.1 Sometimes it is necessary to process information about a person's 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 recognised 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. Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Head of HR.

11. The Data Controller and the Designated Compliance Officer

11.1 The College as a body corporate is the Data Controller under the 1998 Act, and the Board of Governors is therefore ultimately responsible for implementation. However, the Designated Compliance Officer will deal with day to day matters.

11.2 The College has three Designated Compliance Officer: Michael W. Wood, the College Secretary; Veronica Magennis, Executive Officer and Joseph Easson, Registry Manager.

12. Examination Marks

12.1 Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that course fees and other charges have not been paid, or all books and equipment returned to the College.

13. Retention of Data

13.1 The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general, core information about staff and students will be kept permanently (eg for research/archive purposes). This will include:

- date of birth, name, address and matriculation number
- academic achievements
- copies of any references written (if held centrally)

13.2 All other information, including any information about health, race or disciplinary matters will be destroyed within 3 years of the course ending and the student leaving the College.

13.3 The College will need to keep information about staff for a longer period 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.

14. Conclusion

14.1 Compliance with the 1998 Act is the responsibility of all members of the College. Any breach of this Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Compliance Officer/College Secretary.

First Issue: April 2000
Revised: May 2000
Second Revision: May 2002
Revised : October 2004

DPA2002

