

European College of Business and Management

Data Protection Policy

1. INTRODUCTION

- 1.1 The European College of Business and Management (ECBM) is committed to full compliance with the Data Protection Act 1998 [“the Act”] and recognises in full the rights and obligations established by the Act in relation to the management and processing of personal data. This Policy is intended to serve as general guidance for staff and students in implementing the letter and spirit of the provisions and principles of the Act.

2. A BROAD OVERVIEW OF THE ACT

- 2.1 The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them is not processed without their knowledge and is processed with their consent wherever possible.
- 2.2 The introduction of the Freedom of Information Act 2000 amended the Data Protection Act for public authorities, which means that all personal data, and not just that held in a “structured” form is covered by the Act.

3. DEFINITIONS

3.1 Personal Data

Data which relate to a living individual who can be identified from the data, or from the data and other information about the individual which is in the possession of or is likely to come into the possession of the data controller. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2 Personal Sensitive Data

Personal data relating to racial or ethnic origins, political opinions, religious beliefs, union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences and criminal proceedings.

3.3 Data Controller

A person or organisation who determines the purposes for which and the manner in which any personal data, are, or are to be, processed. In ECBM this role is undertaken by the appointed **College Data Protection Officer**.

3.4 Data Processor

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller, (described in the 1984 Act as a computer bureau).

3.5 Data Subject

A living individual who is the subject of the personal data.

3.6 Processing

The obtaining, recording, holding, organizing, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying or otherwise using the data.

3.7 Third Party

Any person other than a data subject or the data controller or any data processor or other person authorised to process data for the data controller or processor.

4. NOTIFICATION

4.1 The Act requires all data controllers to inform (known as notification) the Office of the Information Commissioner of:

- (i) The purpose for which personal data is held or used, e.g. student administration, research, marketing;
- (ii) The types of person for whom personal data is held e.g. students, employees etc. and the class of data e.g. personal identifiers, education records etc.;
- (iii) The source or sources from which the data is obtained and the persons to whom the data may be disclosed;
- (iv) The countries to which data is transferred.

5. THE DATA PROTECTION PRINCIPLES

5.1 The Act contains eight principles, which provide a general framework of duty on the University on how it should process personal data. Personal data should be:

- Processed fairly and lawfully;
- Obtained for one or more specified and lawful purpose(s) and not processed in any manner incompatible with that purpose or purposes
- Adequate, relevant and not excessive for the purpose(s);
- Accurate and up-to-date;
- Not kept for any longer than necessary for the purpose(s);
- Processed in accordance with the data subject's rights;
- Kept safe from unauthorised processing, or accidental loss, damage or destruction;
- Not transferred to a country or territory outside the European Economic Area (EEA) unless that country has equivalent levels of protection for personal data.

6. CONSENT

6.1 In order for personal data to be processed fairly and lawfully, it is essential that the data subject has given his/her consent. This is particularly important if the personal data is classed as "sensitive", as defined under the Act.

6.2 ECBM staff must ensure that consent is always obtained. The most usual methods are by ensuring that there is a data protection statement included on all forms capturing personal data, within guidance notes for the completion of forms, in relevant staff and student handbooks, and on any forms completed on-line.

7. RIGHT OF SUBJECT ACCESS

7.1 The Act gives data subjects the right to access to their personal data held by ECBM. A request must be made in writing (and this includes e-mail requests), and £15 administrative fee paid. This entitles the individual to be told by ECBM whether the College is processing that individual's personal data, the purposes for which they are being processed, to whom they are or may be disclosed and to receive in an intelligible manner, a copy of their personal data.

7.2 ECBM must ensure that it has proof of the identity of the requestor to prevent an unlawful disclosure, and will not release data unless it has that proof.

- 7.3** A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.
- 7.4** ECBM is required by the Act to respond within 40 calendar days of receipt of the request and the fee, but every effort should be made to respond as quickly as possible. The 40 days apply to all requests for personal data, whether routine or complex.
- 7.5** If the request arises as part of another matter for instance, a Personal Mitigating Circumstances [PMC] request, an academic appeal, complaint, grievance or disciplinary matter, the requirements of the DPA must not be overlooked, particularly the 40 day deadline. In these circumstances, staff must seek advice from the Data Protection Officer.
- 7.6** The requested data should normally be provided in permanent form on paper.
- 7.7** If the data subject believes that their personal data is inaccurate, out-of-date, held unnecessarily or is offensive, they have the right to have the information rectified, blocked, erased or destroyed. The data subject also has the right to insist that the College ceases to process their personal data if such processing is causing or is likely to cause unwarranted substantial damage or substantial stress to them or to another. The data subject may also have a right to compensation if it can be proven that damage or distress has been caused.

8. THIRD PARTY DATA AND THE SUBJECT ACCESS RIGHT

- 8.1.** When handling a subject access request, sometimes another individual (known as a third party) may be identified in the personal data to be disclosed. ECBM will only disclose third party data under the Act with the consent of that third party, or if it is reasonable to do so without consent. In determining it whether it would be reasonable, ECBM must balance its duty of confidentiality to the third party against the rights of the data subject; consider any steps taken to seek consent; whether the third party is capable of giving consent; or any express refusal of consent by the third party.

9. EXEMPTIONS

- 9.1** There are a number of exemptions from the provisions of the Act. These allow ECBM to either disclose or withhold data from disclosure in particular circumstances, without breaching the data protection principles.
- 9.2** Guidance on the exemptions and their application can be obtained from the college's Data Protection Officer.

10. GENERAL RESPONSIBILITIES OF ECBM STAFF

- 10.1** When processing personal data, ECBM staff must ensure that they abide by the Data Protection Act, and process data in accordance with the eight data protection principles.

11. SECURITY OF DATA

- 11.1** ECBM staff responsible for processing personal data must ensure that it is kept securely to ensure unauthorised access and only disclose to those authorised to receive it.
- 11.2** In the case of manual data, files containing personal data should be kept in locked storage cabinets when not in use. Such files should not be left on desks overnight.
- 11.3** Electronically held personal data must be protected by a password. Databases should be updated and cleared up regularly.
- 11.4** Any data should be shredded. This applies to personal data like student and personnel paper records as well as to any data concerning ECBM, e.g. teaching material or action plans.
- 11.5** Staff must ensure that they read and understand these policies and procedures.
- 11.6** Care must be taken to ensure that PCs and terminals on which personal data is viewed are not visible to unauthorised persons, especially in public places. Screens showing personal data should not be left unattended. Staff should use the facility “lock computer” on their PC if they are absent from their desk for a short period of time, and should “log-off” for longer periods.

12. RETENTION TIMES

- 12.1** Some legislation provides for minimum periods in which certain types of record must be retained and afterwards shredded. These are
- Student files: 6 years after the student's leaving the college*
- Statutory payments (e.g. Maternity Pay, Sick Pay): 3 years after the end of the financial year to which they relate.*
- All wage/salary records (including those for overtime, bonuses and expenses): 6 years*
- Health and safety records: 2 years (medical records) / 3 years (accident books, records, reports)*
- Application forms, CVs and interview/selection notes of personnel: 1 year*
- Disciplinary and grievance records: 3 years*

Parental leave records: 5 years from the birth/adoption of the child

Pension records: 40 years

Pension trustees' minute books, HM Revenue & Customs approvals, works council minutes and health and safety records of consultations with employee representatives: should be retained permanently

13. DATA PROTECTION ADVICE WITHIN ECBM AND RELATED GUIDELINES AND POLICIES

13.1 The Operations Manager is the Data Protection Officer for ECBM and provides general advice on data protection and freedom of information. The Data Protection Officer should be informed of all data subject requests received by ECBM staff.

Footnote:

THE ROLE OF THE INFORMATION COMMISSIONER

The Information Commissioner is an independent official appointed by the Government to oversee the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Commissioner reports annually to Parliament. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal.

The mission of the Office of the Information Commissioner is to promote public access to official information and to protect personal information.

The Information Commissioner provides good practice guidance and interpretation of the Act for data controllers and advice to the public on how to access personal data. The website of the Office of the Information Commissioner is: <http://www.ico.gov.uk/>

The Commissioner has formal powers to force a data controller to take or refrain from certain actions if the Commissioner has determined there has been or is likely to be a breach of the Act. Failure to comply with a Decision or an Enforcement Notice may be dealt with as though the University had committed contempt of court.