



## DATA PROTECTION POLICY

### 1 Introduction

1.1 The College needs to keep certain information about employees, students and other users to allow it to monitor performance, achievement, and health and safety, for example. 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 complied with. Data includes information held in written records and not just data held on computers. It is a legal requirement that information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the eight Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that personal data must be:

1. Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Adequate, relevant and not excessive for those purposes;
4. Accurate and kept up to date;
5. Not kept for longer than is necessary for that purpose;
6. Processed in accordance with the data subject's rights;
7. Kept safe from unauthorised access, accidental loss or destruction;
8. Not transferred to a country outside the European Economic Area, unless that country has equivalent 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. Breach of the Act can lead to both criminal and civil liabilities. In order to ensure that this does not happen, the College has developed this Data Protection Policy. Further guidance with examples is available in the "Guidelines for complying with the Data Protection Act 1998" document issued to all staff and available on the College's intranet.

### 2 Status of the Policy

- 2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.
- 2.2 Any member of staff who considers that the policy has not been followed in respect of personal data about themselves, should initially raise the matter with the designated Data Protection Officer. If the matter is not resolved, it should be raised as a formal grievance or complaint. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

### **3 Notification of Data Held and Processed**

3.1 All staff, students and other users are entitled to:

- Know 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.

3.2 The College has made a standard form of notification available to all staff, students and other relevant users. This states all the types of data the College holds and processes about them, and the reasons for which it is processed. This is contained in the “guidelines for complying with the data protection act” document which is given to all staff and made available on the College’s Intranet and website.

### **4 Responsibilities of Staff**

4.1 Staff have a responsibility to:

- Check that any information that they provide to the College in connection with their employment is accurate and up to date;
- Inform the College of any changes to information, which they have provided eg changes of address;
- Check the information that the College will send out from time to time, giving details of information kept and processed about staff;
- Inform the College of any errors or changes to information they are responsible for. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

4.2 If and when, as part of their responsibilities, staff collect information about other people, (eg about students’ course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines provided to them.

### **5 Data Security**

5.1 All staff must 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;

5.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5.3 Personal information in the form of manual records should be:

- kept in a locked filing cabinet or:
- locked drawer or:
- other secure area

5.4 Personal information in the form of computerised records should be:

- password protected on the College network; or
- in an area of the College network where access is limited; or
- kept only on a data storage device (such as CD or portable data stick) which is itself secure.

## **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 reception.

6.2 Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify the College's Data Protection Officer. Any student who requires further clarification about this should contact the Data Protection Officer.

## **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 paper files.

7.2 An individual may wish to receive notification of the information currently being held. This request should be made in writing using a standard form available from the Data Protection Officer.

7.3 The College may make a charge for £10 each occasion that access is requested.

7.4 The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided, in the case of staff, within 40 working days and in the case of students, 15 working 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 Information that is already in the public domain is exempt from the 1998 Act. It is the College's policy to make as much information public as possible. The Freedom of Information Act also gives the right to ask any public body for all the information they have on any chosen subject. And unless there's a good reason, they have to provide the information within a month. In order to comply with this act the College has a Freedom of Information Publication Scheme available from the Data Protection Officer or on the College's website:

[http://www.bhasvic.ac.uk/pdf/FOI%20Publication%20Scheme%20\\_external\\_%20.pdf](http://www.bhasvic.ac.uk/pdf/FOI%20Publication%20Scheme%20_external_%20.pdf)

- 8.2 This scheme describes the information that the College intends to publish. However, in addition to this, certain personal data will be available to the public for inspection:
- Names of College governors;
  - Register of interests of Governing Body members and senior staff with significant financial responsibilities (for inspection during office hours only);
  - Lists of staff;

8.3 The College internal phone list will not be a public document.

8.4 Any individual who has good reason for wishing details of these lists or categories to remain confidential, should contact the Data Protection Officer.

## **9 Subject Consent**

9.1 In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **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 Many jobs and courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other legislation 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 members of the College community.

9.3 The College may 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 only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency.

9.4 Therefore, all prospective students and staff will be asked to sign a data protection statement regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

## **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 absence management policy or the Equality and Diversity 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 Data Protection Officer.

## **11 Telecommunications, CCTV and IT infrastructure**

11.1 Computer accounts are the property of the College and are designed to assist in the performance of the work of employees and students. There should, therefore, be no expectation of privacy in any stored work or messages sent or received, whether of a business or of a personal nature.

- 11.2 When sending e-mails on the College's system, the sender is consenting to the processing of any personal data contained in that e-mail and is explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If individuals do not wish the College to process such data, they should communicate it by other means.
- 11.3 The College has the right to monitor any and all aspects of its telephone and computer systems, and to monitor, intercept and/or record any communications made or received by employees, including telephones, email or Internet communications.
- 11.4 Employees and students should be aware that Close Circuit Television (CCTV) is in operation for their protection and the security of College property.
- 11.5 Further information is available in the College's Acceptable Use of Computers Policy

## **12 The Data Controller and the Designated Data Controller/s**

- 12.1 The College, as a body corporate, is the Data Controller under the Act, and the Corporation is therefore ultimately responsible for its implementation. However the Data Protection Officer deals with day to day matters and is therefore the first point of contact for enquirers.

## **13 References**

- 13.1 You should assume that all written or computer stored data (including comments, notes and references) about any student or any member of staff could become disclosed to that person and you should make such comments with this in mind. In particular it should be assumed that all references could be disclosed to the individual about whom the reference is written. Do not assume (unless specific and clear advice is given to the contrary) that a reference headed 'confidential' may not be disclosed to the subject of the reference. (See also the College's policy on writing references.)

## **14 Retention of Data**

- 14.1 The College will keep some forms of information for longer than others. Because of storage restrictions, information about students cannot be kept indefinitely, unless there are specific requests to do so. A list of the archiving retention times employed by the College is included as appendix 1

## **15 Conclusion**

- 15.1 Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the 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 Data Protection Officer.

## **16 Associated policies**

- Child Protection Policy
- Disability Statement
- Disclosure & Confidentiality Policy
- Educational Visits and Out of College Activities Policy
- Staff References Policy and Guidelines

Document history: Approved by the Personnel Committee 6 June 2001 Approved by the Corporation 10 July 2001 Revised June 2007
---------------------------------------------------------------------------------------------------------------------------------------

**Appendix 1**

**RETENTION PERIODS**

<b>Type of Data</b>	<b>Retention Period</b>	<b>Reason</b>
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms; interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20 redundancies)	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more redundancies)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns; correspondence with Tax Office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Accident Books, records and reports of accidents	3 years after the date of the last entry	RIDDOR 1995
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances hazardous to health	40 years	COSHH 1999
Student Records including academic achievements, and conduct	At least 6 years from the last day of the course 10 years with the consent of the student for personal and academic references	Limitation period for negligence