# Data Protection Policy & Procedures

**October 2016**

## Part A INTRODUCTION

### 1 The Data Protection Act 1998

The College needs to keep certain data about its employees, students and other users in order to discharge its duties and realise its strategic objectives. In doing so, the College must comply with the Data Protection Act 1998. This legislation, which came into force on 1st March 2000, defines the rules on how personal data belonging or relating to an individual should be obtained, processed or handled.

The Act gives individuals the right to request to see data which is held on them, and to demand that any inaccuracies are corrected or removed. They also have the right to be told whether personal information relating to them is being processed and for what purposes.

### 2 Glossary of terms used in the Act

2.1 'Data' is information which:

- 'is being processed by means of equipment operating automatically in response to instructions given for that purpose' or 'is recorded with the intention that it should be processed by means of such equipment'
- is recorded as part of a 'relevant filing system' or with the intention that it should form part of a 'relevant filing system'
- forms part of an 'accessible record'. 'Accessible record' is defined to include health records relating to the physical or mental health or condition of an individual made by, or on behalf of, a health professional in connection with the care of the individual concerned

2.2 'Personal data' includes all data about a living individual who can be identified from the information. It includes any expression of opinion about the individual and any indication of the intentions of the employer or any other person in respect of the individual.

2.3 'Sensitive data' is given special protection and is defined as personal data, which relates to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual preferences and criminal convictions.

2.4 The Act applies to data stored in a 'relevant filing system', defined as a set of information in which records are structured so that 'specific information relating to a particular individual is readily accessible'. This means that a substantial amount of manual data (i.e. information held on a personnel file) will fall within the scope of the Act. Information not held centrally but kept for example by line managers will also be covered by the Act.

2.5 'Processing' takes in 'obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data'. This includes organisation, adaptation, alteration, retrieval, consultation, use, disclosure by transmission or dissemination, alignment, combination, blocking erasure or destruction of the information or data.

2.6 A 'Data controller' is 'a person who, whether alone or jointly or in common with other persons, determines the purposes for which and the manner in which any

personal data are, or are to be, processed.

## 3 The Data Protection Principles

Anyone processing data belonging, or relating, to an individual must comply with the **eight** enforceable principles of good practice. Data must be:

- fairly and lawfully obtained and processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept for longer than is necessary
- processed in accordance with the individual's rights
- kept safe from unauthorised access, accidental loss or destruction
- not be transferred to countries without adequate levels of protection for personal data

## PART B THE PROCEDURE

## 4 How does the Data Protection Act (1998) affect individuals within the College?

The College is registered under the Act which is designed to protect employees, students and other users. Personal data, which covers all data held manually and on computer systems, will be collected in a fair and lawful way. It will only be held for specific and lawful purposes in relation to the individual's association with the College and will not be disclosed inappropriately. Personal data will be kept up to date and deleted when no longer relevant.

## 5 What are an individual's rights?

5.1 All employees, students and other users are entitled to:

- know what the College is doing to comply with its obligations under the 1998 Act
- know what information the College holds and processes about them and why
- know how to gain access to it
- have access to, or right to request a copy of, manual information and have a copy of the data held by the College relating to them
- view data held electronically about the individual
- demand that any inaccuracies are corrected or removed
- compensation where breach of the Act has caused damage

The arrangements that apply to the access of personal data are given in section 7.

5.2 The College will provide all employees, students and other relevant users with a standard form of notification (see section 9).

5.3 By signing any of the documents below, an individual authorises the College to use information in accordance with the regulations:

- Contract of Employment (employees). This may include the provision of

personal information to the employee's line manager, but this will only be in connection with their employment with the College.
- Acceptance of a place on a study programme at the College (students, parents or guardians).
- Specific contracts for the provision of works and services (contractors).
- Letting forms (those individuals wishing to hire out College facilities and equipment).
- In relation to the operation of the Corporation (Governors).

5.4 Sometimes it is necessary to process 'sensitive data' on an individual, as defined in section 2.3, in order to ensure that the College is a safe place for everyone, or to operate other College policies, such as the Sickness Absence Policy or Equality Policy. Since this information is considered sensitive, the individual will be asked to give written consent for the processing to be carried out. An offer of employment or a place on a study programme, at the College may be withdrawn if an individual refuses to consent to this, without good reason.

5.5 The processing of 'sensitive' data will only be exempt from the individual's consent where the need to process is urgent, for example, where a delay could lead to serious injury or loss of life.

5.6 The Police Act 1997 allows for the establishment of a system of criminal conviction certificates, which may be requested by employers, in relation to employment with children and vulnerable adults. Under this Act, and as a condition of appointment, the College will carry out checks in relation to an individual's criminal conviction.

## 6 What are an individual's responsibilities?

6.1 All employees, students and other users are responsible for:
- checking that any information that they provide to the College is accurate and up to date
- informing the College of any changes to the information which they have provided. The College cannot be held responsible for any errors unless the individual has informed the College of them
- checking any information that the College may send out from time to time, giving details of the information kept and processed about the individual
- ensuring that any personal data that they hold is kept securely and that it is not disclosed either orally or in writing to any unauthorised third party

6.2 It should be noted that unauthorised disclosure will usually be dealt with as a disciplinary matter and may be considered to be gross misconduct.

## 7 How does an individual get hold of the data held on them?

7.1 Employees, students and other users of the College have the right to request access to any personal data that is being kept about them, whether this be held in manual files or on computer.

7.2 An individual who wishes to exercise this right should complete the College's 'Request Form for Access to Personal Data', available from, and returnable to, the Data Protection Officer. The form must be accompanied by an

administration fee of £10 to cover the cost of copying and forwarding the information.

7.3 The personal data will be sent to the applicant within 40 days of the request, beginning on the day that the Data Protection Officer receives the request and the administration fee.

7.4 The following conditions apply to the disclosure of personal information:

- The College will not comply with repeated requests for disclosure unless these are made at reasonable intervals.
- There is no right of access to confidential information processed for: (i) management forecasting or planning purposes, or (ii) negotiations with the individual or (iii) confidential communications between the College and its legal adviser.
- There is no right of access to personal data where the information would reveal the identity of a third party unless: (i) the third party consents, or (ii) it is reasonable in all circumstances to dispense with the third party's consent, or (iii) the third party is a health professional who has compiled/contributed to a health record.
- There is no right of access to confidential references (in relation to education, training or employment) given by the College.
- An individual may only have access to a reference from a third party where either the College receives the third party's consent to the disclosure of the reference or it must be reasonable in all circumstances to do so.

## 8 What happens if the data supplied to an individual is incorrect or out of date?

8.1 If, having received the information held, an individual discovers that the data is inaccurate or out of date, they should write to the Data Protection Officer stating the inaccuracies. As much information as possible should be supplied, together with details of the correct information. The individual should retain a copy of this letter.

8.2 On receiving the request, the Data Protection Officer, in conjunction with the Student & Pastoral Support Manager in the case of students or the Personnel Officer in the case of employees, will investigate the inaccuracies and make any amendments to the data, as necessary. The Data Protection Officer will then write to the individual either informing them that the changes have been made or giving the reason why changes have not been made. Such a response will be made within 40 days of the written request that the inaccuracies should be investigated.

8.3 If, at an individual's request, the College refuses to remove the data, the individual can ask the Data Commissioner to intervene. Under Section 14 of the Act, an individual also has the right to apply to the High Court or county court for an order requiring the College to correct inaccuracies in data.

## 9 Data Controller and Notification

9.1 The College as a body corporate is the Data Controller under the Act, and the Corporation is therefore ultimately responsible for implementation. However, the 'designated' Data Controller is the Data Protection Officer, and s/he will deal with matters on a day to day basis.

9.2 The Data Protection Act requires that every data controller who is processing personal data needs to notify the Information Commissioner by means of a Registration. The College's register entry includes the name and address of the Data Controller and a general description of the processing of personal data by the Data Controller. The Data Protection Public Register website (www.dpr.gov.uk) has a complete copy of the public register, updated weekly.

## 10 Retention of Data

The College will retain categories of data for different lengths of time but, due to the limitation on storage space, data cannot be kept indefinitely, unless there are specific requests to do so. In general, data will be retained for the following maximum periods of time:

| | | |
|---|---|---|
| Manual data: | employees | 2 years |
| | students | 6 years |
| | others | 6 years |
| Electronic data: | all data subjects | kept for alumni and job reference purposes |

Allegations of Abuse Against Staff

It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future DBS Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer.

## PART C RESPONSBILITIES OF STAFF

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. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

2. If and when, as part of their responsibilities, staff collect information about other people's opinions about ability, references, or details of personal circumstances, they must comply with the appropriate guidelines for staff.

**Data Security**

3. 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.

4. Personal information should be;
   - kept in a locked filing cabinet; or
   - in a locked drawer; or
   - if it is computerised, be password protected; or
   - when kept or in transit on portable media the files themselves must be password protected

5. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the Deputy Principal must be obtained. Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites, **unless the data has been encrypted using appropriate software.**

6. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:
   - suitable backups of the data exist
   - sensitive data is appropriately encrypted
   - sensitive data is not copied onto portable storage devices without first consulting the Network Manager in regard to appropriate encryption and protection measures
   - electronic devices such as laptops that contain sensitive data are not left unattended when offsite

7. For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Principal.

Last Reviewed: October 2016
Next Review date: October 2019

**Appendix 1**

**Staff Handbook: Data Protection 'Key Points' for Employees**

1. Most information that you will deal with on a day-to-day basis will be classified as 'personal data', that is, data about a living individual who can be identified from the information. It includes any expression of opinion about the individual and any indication of the intentions of the College, or any other person, in respect of the individual. This would include matters relating to performance, behaviour and discipline.

2. 'Sensitive data' is given special protection and is defined as personal data, which relates to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual preferences and criminal convictions. If you need to process 'sensitive' data, you must obtain the individual's written consent, except where the need to process is urgent, for example, where a delay could lead to serious injury or loss of life.

3. In processing data, you must particularly ensure that it is accurate, up to date, fair, kept securely and disposed of safely.

4. Before processing any data about an individual, employees should consider the following checklist:
   - Do you really need to record the data?
   - Has the individual been told that this type of data will be processed?
   - Is the data 'personal' or is it 'sensitive'?
   - If it is 'sensitive', do you have the individual's express consent to process?
   - Are you authorised to process this data?
   - If yes, have you checked with the individual that the data is accurate?
   - Are you sure that the data is kept securely?
   - Are you disposing of out of date data safely, e.g. by shredding it?

**Appendix 2**

**Request Form for Access to Personal Data**

I, _____, wish to have access to either [delete 1. or 2. as appropriate]

1. All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or

2. Data that the College has about me in the following 'ticked' categories:

   - ☐ Personal details
   - ☐ Health and medical matters
   - ☐ Political, religious or trade union information
   - ☐ Academic or employment references
   - ☐ Any statements of personal judgement about my abilities or performance
   - ☐ Appraisal summaries
   - ☐ Behaviour or disciplinary issues
   - ☐ Academic marks or coursework details
   - ☐ Other information (please detail below)

     _____
     _____
     _____

I attach a payment of £10 to cover the cost of copying and forwarding the information.

Signed _____

Date _____

**When completed, this form should be passed to the Data Protection Officer who will respond to you within 40 days of its receipt.**