Data Protection Policy

1. Introduction

1.1 The College needs to keep certain information about its employees, students and other stakeholders, for example 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 complied with. 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. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose and shall not be 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 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. In order to ensure this the College has developed this Data Protection Policy.

2. Scope of this policy

2.1 This policy does not form part of the formal contract of employment but it is a condition of employment that **all** employees will abide by the rules and policies made by the College from time to time. Any failures 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 must immediately raise the matter with the Data Protection Officer (see paragraph 14.)

3. Data Protection Officer

3.1 The College is required to nominate a Data Protection Officer to oversee our compliance with the Data Protection Act 1998. The Data Protection Officer is the Vice Principal Finance and Resources.

3.2 The role of the Data Protection Officer is to

- **Develop and implement the College's Data Protection Policy**
- **Provide information and guidance on the processing of all personal data**
- **Ensure staff receive appropriate training**
- **Process, co-ordinate and respond to all requests for information.**

4. Notification of data held and processed

All staff, students and other stakeholders are entitled to know:

- What information the College holds and processes about them and why
- How to gain access to it
- How to keep it up to date
- What the College is doing to comply with its obligations under the 1998 Act.

5. Responsibilities of staff

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

6. Data security

6.1 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.

6.2 Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 6.3 to 6.7 below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

6.3 Personal information should be kept in a locked filing cabinet or in a locked drawer. If it is computerised it should be password protected and when kept or in transit on portable media the files themselves must be password protected.

6.4 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.

6.5 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 **Data Protection Officer** must be obtained, and all the security guidelines given in this Policy must be followed.

6.6 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 data exist
- Sensitive data is appropriately encrypted
- Sensitive data is not copied onto portable storage devices without first consulting the **Data Protection Officer** in regard to appropriate encryption and protection measures

- Electronic devices such as laptops, mobile devices and computer media (USB devices, CDs etc) that contain sensitive data are not left unattended when offsite.

6.7 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 **Data Protection Officer.**

7. Student obligations

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 College promptly.

8. Rights to access information

8.1 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 contact the Vice Principal Finance and Resources.

8.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing. The College will make a charge of £10 on each occasion that access is requested.

8.3 The College aims to comply with requests for access to 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 the delay will be explained in writing to the data subject making the request.

9. Publication of College information

Please refer to the College's Freedom of Information Guide which can be found on the College's website.

10. Information Supplied to External Bodies

10.1 Details contained within a student's record will be passed to the central government departments and agencies, such as the Skills Funding Agency (SFA), which require them in order to carry out their statutory functions.

10.2 This data is used for a variety of purposes including the operation of the Further Education funding methodology whereby funds are distributed by the SFA/Education Funding Agency (EFA) to the College.

10.3 Under the Data Protection Act 1998 students have the right to know what information is held about them by such agencies as the SFA. Students should contact the Vice Principal Finance and Resources to discuss this matter further.

11. Subject consent

11.1 In many cases, the College can only process 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 of staff. This includes information about previous criminal convictions.

11.2 Some jobs or courses will bring the applications into contact with children, including young people between the ages of 16 and 18. The College has a duty of care under the Children 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.

11.3 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 and 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, for example.

12. Processing sensitive information

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 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.

13. Examination marks

Students will be entitled to aggregate 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 the full course fees have not been paid, or all books and equipment returned to the College.~~

14. Retention of data

The College will keep some forms of information for longer than others. Because of storage problems, information cannot be kept indefinitely. In general information about students and staff will be kept a maximum of six years after they leave the College. Section 4 of the College's Financial Regulations refers to document retention and includes a link to the JISC Retention Schedule for Further Education and should be read alongside this document.

15. Status of this Policy

15.1 This policy was approved by SMT in **May 2015**.

15.2 The operation of this policy will be kept under review by the Senior Management Team.

Date approved:	September 2014
Approved by:	SMT
Date reviewed:	**May 2015**
Date of next review:	**May 2017**

Appendix: Response to a breach of data protection

1. **If a member of staff becomes aware of a breach or suspected breach of data protection they must immediately advise the Data Protection Officer of the breach and the date and time when the breach or suspected breach occurred.**
2. **The Data Protection Officer will**
    - **take necessary steps to ensure there are no further breaches**
    - **document everything known thus far about the breach; including who discovered/reported it, what the breach was, what systems or devices are affected**
    - **review processes and procedures with a view to reducing the risk of the breach reoccurring**
    - **assess any training needs identified**
    - **produce a written report.**
3. **An electronic copy of the Data protection Officer's report will be retained in the SLT folder.**