

Introduction

The College needs to keep certain information about employees, students and other users to allow it to monitor performance, achievements, and Health & 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. To comply with the law, information must be 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 shall not be processed unless certain conditions are met.
- Be obtained for a specified 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.

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.

Status of the Policy

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.

Staff and Student Concerns Regarding College Compliance with the Policy

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Designated Staff Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Any student who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Designated Student Data Controller initially. If the matter is not resolved it should be raised as a formal complaint.

Notification of Data Held and Processed

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.

The College will therefore provide all staff and students and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them, and the reasons for which it is processed. The College will try to do this annually. Forms of data held include paper records, computerised information, digital records and video recordings from the College's security surveillance systems.

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 or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.
- Informing the Designated Staff Data Controller of any new data systems being developed.

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

Data Security

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.

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

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 secure.

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 relevant Cluster Administration Office.

Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify the Designated Student Data Controller. Any student who requires further clarification about this should contact the Designated Student Data Controller.

Rights to Access Information

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 complete the College 'Standard Request Form for Access to Data' and hand it in to Reception, who will forward it to the appropriate Designated Data Controller.

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 using the standard form attached.

The College will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 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.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is College policy to make as much information public as possible. Details are set out in the Policy on Access to College Information, which is available on request from the Designated College Data Controller.

Subject Consent

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.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 18. The College has a duty 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.

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 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.

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

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race, 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, diversity and race relations 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.

Examination Marks

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 the full course fees have not been paid, or all books and equipment returned to the College.

Retention of Data

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. A list is attached of the archiving guidelines and retention times employed by the College.

The Data Controller and the Designated Data Controller/s

The College as a body corporate is the Data Controller under the 1998 Act, and the Corporation is therefore ultimately responsible for implementation. However, the Corporation has delegated to the Designated College Data Controller responsibility for dealing with day to day Data Protection matters. The Designated College Data Controller is:

Jim Edwards , Room 4.25, North Building, City College Coventry, 50 Swanswell Street, Coventry, CV1 5DG, tel 024 7679 1530, email j.edwards@covcollege.ac.uk who may either deal with the enquiry himself or refer it to another Designated Data Controller.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate 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 Designated College Data Controller.

Contribution to Achievement of the College's Mission

The College's Mission is '*Promoting to Diversity, Raising the Standard, Taking Education Further*'. This Policy contributes to the Mission by ensuring the highest standards in its Data Protection arrangements.

Monitoring and Impact Measurement

The effectiveness of the Data Protection Policy will be monitored regularly by the Designated College Data Controller subject to annual review by the Executive. The effectiveness of this policy will be measured by the number of instances in which it is invoked or breached, and the actions taken in response. The policy will be reviewed annually.

Publication of Policy

This policy will be made publicly available and provided to all members of staff via the Intranet.

Policy Review Date	March 2012
Executive member responsible for implementation	Director of Estates

Approval and Review History
• Approved by the Corporation on 17th September 2003 (Minute C77/03)
• Reviewed and approved by the Corporation on 15th September 2004 (Minute C73/04)
• Reviewed and approved by the Corporation on 14th September 2005 (Minute C71/05)
• Reviewed and approved by the Corporation on 13th September 2006 (Minute C72/06)
• Reviewed and approved by the Corporation on 5th December 2007 (Minute C102/07)
• Reviewed and approved by the Principal (under delegated authority from the Corporation) at the Executive meeting of 23rd November 2009 (Minute X)
• Reviewed and approved by the Principal (under delegated authority from the Corporation) at the Executive meeting of 19th March 2012