

| | | |
|--|---|---------------|
| Title | Data Protection Policy | |
| Aim | To state the College's policy and to outline the College's approach to data protection | |
| Related Policies / Documents / Procedures | <p>The Data Protection Policy is related to many of the College's other policies, but in particular to:</p> <ul style="list-style-type: none"> • Whistleblowing Policy • Acceptable Computer Use Policy | |
| Date for Implementation | March 2008 | |
| Approved by | Board of Governors | 14 March 2008 |
| Date of next review | March 2011 | |
| Distribution | <p>Leadership Team All College staff</p> | |
| Version Control | Previous Versions approved: | |

Data Protection Policy

1. Introduction

The Co-operative College holds information about its board members, employees, learners, partner organisations, suppliers and other users as a normal part of its day-to-day business. It is necessary for example to process information so that staff can be recruited and paid, learners enrolled, courses organised, awards and assessments held and legal obligations to funding bodies and government complied with.

The Data Protection Act 1998 came into force on 1 March 2000. This Act introduces significant new responsibilities that the College must take account of.

The purpose of the Act is to ensure that data is collected and used in a responsible and accountable manner and to provide the individual with a degree of control over the use of their personal data. To comply with the law information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

It is the intention of the Co-operative College to comply with the terms of the Data Protection Act 1998. The College will ensure that the interests of its employees and learners are safeguarded by regularly reviewing its policy and taking account of Codes of Practice and other advice issued by the Information Commissioner. It will also take account of the wider legal framework introduced by the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998 and the Freedom of Information Act 2000.

The Co-operative College and all staff or others who process or use personal information must ensure that they follow the Data Protection Principles at all times. In order to ensure that this happens, the Co-operative College has developed the Data Protection Policy.

The Co-operative College acknowledges that the College or individual members of staff may be held liable for criminal offences under the Data Protection Act 1998. Fines for breaches are unlimited.

2. The Data Protection Act 1998

The 1998 Act places duties and obligations on Data Controllers in relation to their processing of personal data. Personal data includes information about living, identifiable individuals (data subjects) that is to be processed by means of automated equipment (including computer processing). This may include emails which are processed with reference to the data subject.

Personal data also includes information recorded as part of a relevant filing system. This is any manual filing system, microfiche or paper set of information that is

structured in such a way that information relating to a particular individual is readily accessible.

Personal data must be processed fairly and lawfully. There must be a clear purpose for processing.

Processing means obtaining, recording, holding or carrying out any operation on the information or data.

Sensitive personal data is a special category. It may only be processed with the explicit consent of the data subjects:

- The racial or ethnic origin of the data subject.
- Political opinions.
- Religious or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- The commission or alleged commission of any offence.
- Proceedings for any offence or alleged offence.

Data Protection Principles state that personal data must be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Adequate, relevant and not excessive.
4. Accurate.
5. Not kept for longer than is necessary.
6. Processed in accordance with individuals' rights.
7. Secure.
8. Not transferred to countries without adequate protection.

Rights for Individuals under the Data Protection Act 1998:

- Right of subject access (to data held on computer records and relevant filing systems upon making a request in writing and paying a fee).
- Right to prevent processing likely to cause unwarranted and substantial damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Right to compensation.
- Right to correction, blocking, erasure or destruction.
- Right to ask the Information Commissioner to assess whether the DPA has been contravened.

Criminal Offences under the Data Protection Act 1998:

- Processing without notification.
- Failure to comply with an enforcement notice.
- Unlawful obtaining or disclosure of personal data.

- Selling or offering to sell personal data without the consent of the data subject.

3. Status of the Policy

This policy is a broad summary of the Co-operative College's responsibilities under the Data Protection Act.

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 Co-operative College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

4. Co-operative College Compliance Framework

The College, as a body corporate, is the Data Controller under the Act and the Corporation is therefore ultimately responsible for implementation.

The designated Data Controllers on behalf of the College are:

- Head of Finance and Corporate Services
- Director of Learning and Development

The Data Controllers are responsible for data within their normal line management responsibility within the College.

The Data Protection Officer on behalf of the College is:

- Head of Management Services

A copy of the Data Protection Policy will be held on the College website. A full paper copy will be available from the Head of Management Services and in the Employee Handbook.

5. Responsibilities of Staff

The College will require all staff to familiarise themselves and comply with the Data Protection Policy.

6. Responsibilities of Learners

The College will require all learners to consent to processing under the Data Protection Act and to comply with the Data Protection Policy.

7. Notification of Data held and processed

All staff, learners and other users are entitled to:

- Know what information the College 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.

8. Conditions for Processing

Authorised processing of information takes place as part of the day-to-day business of the College in accordance with the schedule in the Co-operative College Data Protection Act Notification.

Conditions for authorised processing may include:

- Consent of the data subject.
- Necessary for the legitimate interests of the Co-operative College or by third parties to whom the data is disclosed except where processing is unwarranted because of prejudice to legitimate interests of the data subjects.
- Necessary for a contract with the data subject.
- Necessary to protect the vital interests of the data subject.
- Necessary for the administration of justice.
- Necessary for any enactment.
- Necessary function of a Crown Minister, or government department necessary functions of a public nature exercised in the public interest.

9. Subject Access Rights to Information

Employees, learners and other users of the College have subject access rights to certain personal data that is being held about them either on computer or in manual files. Any person who wishes to exercise this right should put their request in writing.

Subject access requests for staff and learners should be made in writing to the Head of Management Services.

The data subject must supply sufficient information to enable the College to locate the information that the subject seeks. The College is not obliged to comply with open ended requests. The College may refuse to disclose data that makes reference to the personal data of third parties.

The College will make a standard charge of £10 on each occasion that access is requested, although the College has the discretion to waive this.

The College aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within 40 calendar days unless there is good reason for the delay. In such cases, the reason for delay will be explained in writing to the data subjects making the request.

10. Disclosure of Personal Data

Disclosure of data to authorised recipients takes place as part of the day to day business of the College. Authorised disclosure will take place according to the schedule in the Co-operative College Data Protection Act Notification.

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Particular discretion must be used before deciding to transmit personal data by fax or email.

Where non routine requests are made or where staff are unsure of their responsibilities they should seek the advice of their line manager. The line manager may decide to refer a request for a definitive decision to the Data Controller who holds responsibility for their areas of line management or to the Data Protection Officer. The Data Protection Officer will provide advice about the interpretation of the Act.

Staff should be aware that those seeking information about individuals may use deception to obtain information. Staff should take steps to verify the identity of those seeking information, for example by obtaining the telephone number and returning the call or by reviewing identification documents if an application is made in person. All applications for data should be made in writing.

Request by the other public bodies, including the police, must meet the requirements for lawful processing. The police must be able to demonstrate that they require the information in pursuit of a criminal investigation.

Where a disclosure is requested in an emergency, staff should make a careful decision as to whether to disclose, taking into account the nature of the information being requested and the likely impact on the subject of not providing it.

11. 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 learner onto any course, and a condition of employment for staff.

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

to ensure staff are suitable for the job, and learners for the courses offered. The College also has a duty of care to all staff and learners and must therefore make sure employees and those who use the College do not pose a threat or danger to other users. Where appropriate therefore the College will obtain information about previous criminal convictions.

The College will notify all users at the point where information is collected from them which information will be processed and the purpose of processing under the Data Protection Act. The consent of the user will be obtained at the point of collection. This includes;

- Application forms for Board of Management members.
- Application forms for staff.
- Registration forms for learners.

The College will also ask users to consent to receive promotional details about additional activities and further study opportunities which may be of interest to them. Users have a right to decline receipt of this information.

The College will also ask learners if they wish to consent to the College, DCSF, DIUS, awarding bodies or their employer/sponsor using their data for follow-up activities.

12. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender or family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the 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 learners 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. 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, and in particular the following information will be available to the public:

- Names of Board of Management members, details of application to become a board member and register of interests.
- Names and positions of senior post holders and register of interests.

Any individual who has good reason for wishing details to remain confidential should contact the designated data controller.

14. 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 know that unauthorised disclosure may be regarded as a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:

- Kept in a locked filing cabinet or locked drawer.
- If it is computerised, be password protected.

Particular care must be taken with data held on portable disks or laptop computers.

Staff should ensure that casual disclosure does not take place by for example leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens.

Computer printouts must be kept securely and shredded when no longer required.

Special consideration should be given to prevent unauthorised access to data in offices where staff are employed to process personal data.

Staff should take particular care with data processed while working at home.

15. Retention of Data

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements.

Standard retention times for finance related documents are specified in the College Finance Regulations. Retention times for other categories of data are specified in the College Document Retention Policy.

| | |
|-----------------------------|------------------------|
| Application form | Duration of employment |
| References received | 1 year |
| Payroll and tax information | 6 years |
| Sickness records | 3 years |
| Annual leave records | 2 years |

| | |
|---|--|
| Unpaid leave/special leave records | 3 years |
| Annual appraisal/assessment records | 5 years |
| Records relating to promotion, transfer, training, disciplinary matters | 1 year from end of employment |
| References given/information to enable references to be provided | 5 years from reference/end of employment |
| Summary of record of service, eg name, position held, dates of employment | 10 years from end of employment |
| Records relating to accident or injury at work | 12 years |

16. Disposal of Data

Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records which are part of the formal College records system.

This material must not be disposed of in ordinary office waste paper bins.

Personal data must be destroyed by secure methods such as shredding.

17. References

The provision of a reference will generally involve the disclosure of personal data. The College is responsible for references given in a corporate capacity. All staff references requested should be referred to the Head of Management Services or Head of Learning and Development. All references provided in a corporate capacity about employees and learners will incorporate a standard disclaimer paragraph agreed by the College.

The College is not responsible for references given in a personal capacity. These must not be provided on Co-operative College stationery and should be clearly marked as personal.

The College will not provide subject access rights to confidential references written on behalf of the College about employees and learners and sent to other organisations. This is a specific exemption allowed by the Act.

The College recognises that once the reference is with the organisation to whom it was sent then no specific exemption from subject right access exists.

The College will normally provide subject right access to confidential references received about employees and learners provided to the College by other organisations. However the College may withhold information if it is likely to result in harm to the author or some other person or if it reveals information about another third party other than the previous supervisor or manager of the employee.

18. Direct Marketing

The College will only use personal data for promotional campaigns or to market additional activities to existing or previous learners where they have given consent. Any staff wishing to send out marketing material to learners such as details for further course opportunities must check on the learner database to verify that the learner has consented.