Data Protection Policy

www.weston.ac.uk

Construction Training Centre, Locking Head Drove, Weston-super-Mare, BS24 7NA
T: 01275 465 555 **E:** info@somax.eu.com **www.**construction-training-centre.co.uk

INTRODUCTION

The Data Protection Act 1998 came into force on 1st March 2000. 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 Weston College to comply with the terms of the Data Protection Act 1998. 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, Weston College has developed the Data Protection Policy and is registered for Notification under the Act.

The College holds information about its Corporation members, employees, students, partners, suppliers and other users as a normal part of its day-to-day business. The College will ensure that the interests of its employees and students 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 and their impact in respect of Data Protection.

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

INTERPRETATION OF THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 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 and CCTV images). This may include e-mails 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.

www.weston.ac.uk

Core 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 Data Protection Act

  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.

  Core 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 Data Protection Act

  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.

A FRAMEWORK FOR COMPLIANCE

The College, as a corporate body, 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:

 ICT Manager, MIS Supervisor, HR Manager, **Head of** Customer Services, College Accountant

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:

 MIS Manager

The Data Protection Officer will be responsible for convening a Data Protection team. The Data Protection Team will be responsible for:

- Data Protection Policy.
- The Data Protection Notification.
- Review of procedures.
- Data Protection audits.

RESPONSIBILITIES OF STAFF

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

RESPONSIBILITIES OF STUDENTS

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

RESPONSIBILITIES OF CONTRACTORS & PARTNERS

A Data Protection Memorandum of Understanding will be included in all contracts where third parties process data on behalf of the College and where third parties have access to data as a necessary part of their contracted work.

NOTIFICATION OF DATA HELD AND PROCESSED

All staff, students 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

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 College Data Protection Act Notification. Conditions for authorised processing may include:-

- consent of the data subject
- necessary for the legitimate interests of the 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

SUBJECT ACCESS RIGHTS TO INFORMATION

Employees, students 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 should be made in writing to the Head of Human Resources. Subject access requests for students should be made in writing to the **Head of** Customer Services.

Any other requests should be made in writing to the Data Protection Officer. 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.

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 College Data Protection Act Notification which is located on the College Intranet.

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Personal data relating to students under the age of 18 will only be disclosed to the parent with whom the person resides. Any requests for information from absent parents will require the consent of the student in question.

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 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 and e-mail requests will be accepted.

Request by 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.

Disclosure Of Data To Employers

Many students attend college under the sponsorship of their employers. This may include paid time to attend or payment of fees. These students will be required to consent to the sending of routine reports to their employers on academic progress and attendance as part of their “Data Protection Consent to Process” on the application and enrolment form.

Students Below The Age Of 18

Parents and carers of young people attending College below the age of 18 do not have automatic rights under the Data Protection Act to information about their children. It is important to ensure appropriate communication between the home and the College. Students below the age of 18 will be required to consent to sending of routine reports on academic progress and attendance as part of their "Data Protection Consent Process" on the application and enrolment form.

Other non-routine requests for information from parents or carers should be considered carefully. It should be normal procedure to request permission from the student before disclosing any additional information.

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.

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 students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure employees and those who use the College facilities 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 Corporation members
- Application forms for staff
- Application forms for students
- Enrolment forms
- Telephone enquiries and applications
- Internet enquiries/e-mail, applications and enrolments

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

The College will ask students below the age of 18 to consent to disclosure of information to parents and carers.

The College will ask students to consent to disclosure of information to employers, where students are sponsored by employers to attend college.

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. 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.

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. Types of information available are recorded in the College's Publication Scheme in compliance with the Freedom of Information Act 2000.

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. Personal information should be:

- Secured in a locked filing cabinet or desk 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 destroyed in a confidential manner.

College offices where staff are employed to process personal data should be locked when not occupied.

Staff should take particular care with data that has been processed while working at home. All staff and students are responsible for ensuring that they observe the procedures of other appropriate College policies.

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 related documents are specified in the College's Financial Regulations which can be located on the College Intranet.

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.

Personal data must be destroyed by secure methods such as shredding or confidential waste sacks handled by authorised contractors.

Formal records may only be destroyed with the appropriate authority.

STUDENT UNION DATA

The College is not responsible for data held by the Student Union. However the College will provide guidance to the Student Union as to their responsibilities under the Data Protection Act.

EXAMINATION RESULTS

Students will be entitled to information about their marks for both coursework and examinations. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or books and equipment have failed to be returned to the College. Examination results may be made available for publication in the local newspapers. The College does not have to obtain specific consent to publish results but students have a right to object to publication. News stories focussing on individual students will only be made available with the consent of the student.

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.

The College is not responsible for references given in a personal capacity. These should never be provided on Weston 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 students 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 students provided to the College by other organisations. However, the College may withhold information under the auspices of the Act; as deemed appropriate.

CCTV

CCTV systems must be positioned to avoid capturing images of persons not visiting College premises. The recorded images must be stored safely and only retained long enough for any incident to come to light. Recordings will only be made available to law enforcement agencies, and approved College personnel, involved in the prevention and detection of crime and to no other third party.

DIRECT MARKETING

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

POLICY REVIEW

This policy shall be reviewed every 2 years.

This policy was approved by the Corporation on 25 May 2006