



Data Protection Policy

Issue	January 2009
Review Date	July 2009
Originator	Anthony Robertson Vice Principal Corporate Services
Location of Policy	Intranet/Policies & Procedures/Corporate

1. Background

The Data Protection Act applies to personal data which is defined as information relating to identifiable living individuals. It gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly by those responsible for obtaining, holding or otherwise processing it. Under the Act, processing is defined very broadly and includes the collection, retention, use and disclosure of information

The Act works in two ways. Firstly, it sets out 8 principles and requires that anyone responsible for processing personal data must comply with these principles. The 8 Data Protection Principles are that personal data must be:

- processed fairly and lawfully
- processed only for specified purposes
- adequate, relevant and not excessive
- accurate and up to date
- kept for no longer than is necessary
- processed in line with the rights of individuals to whom the data relates
- kept safe from unauthorised access, damage, accidental loss or destruction
- transferred to countries outside the European economic area only where there is adequate protection for the privacy of the individuals concerned

Secondly the Act provides individuals with important rights, including the right to find out what personal information the College holds about them. Rights for individuals under the Data Protection Act 1998 include:

- right of subject access (to all recorded personal information held by the College, irrespective of its format, unless an exemption applies, provided it is requested in writing and a fee has been paid)
- right to object to processing likely to cause unwarranted and substantial damage or distress
- right to compensation in certain circumstances
- right to prevent processing for the purposes of direct marketing
- right to correction, blocking, erasure or destruction of incorrect records
- right to ask the Information Commissioner to assess whether the DPA has been contravened

Individuals who feel they are being denied proper access to their personal information or feel this information is not being handled according to the eight principles, can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

Failure to comply with the Data Protection Act 1998 will, in some instances, constitute a criminal offence.

Criminal offences under the Data Protection Act 1998 include: -

- processing without notification (see section 6.1 of this policy)
- failure to comply with an enforcement notice issued by the Information Commissioner
- unlawful obtaining or disclosure of personal data
- selling or offering to sell personal data without the consent of the data subject

2. Context

Swansea College needs to collect, process, keep and use certain types of information about people with whom it deals in order to carry out its day to day functions. These people include current, past and prospective students, customers, staff, partners, Corporation members, suppliers of goods and others. This personal information, whether on paper, on a computer, or recorded on other material, must be used fairly and processed in accordance with the Data Protection Act 1998. The data must also not be disclosed to any other person unlawfully.

All staff & students should be aware: -

- that all **personal data** collected, held, and processed (including via www tools and other Internet software) whether in manual, digital, electronic or any other format is **subject to the Data Protection Act**
- of the circumstances under which they may or may not legitimately **access, process and disclose personal data**

Note – Individuals, including staff and students, in relation to whom the College holds information are referred to in this policy as **“data subjects”**

The College’s **Data Controllers** for the purposes of this policy are: -

Dave Hibbs – Director of Data College Management - student related data enquiries

Nicola Perkins – Director of Human Resources – staff related data enquiries

3. Scope

This policy applies to all staff & students in the College and should be read in conjunction with the College’s Data protection Guidelines for Staff which provides detailed guidance on the application of the Act & Policy in specific circumstances.

This policy applies to all information/data relating to living individuals that is collected, processed and stored by the College.

This policy applies to requests by individuals for information about themselves as well as to specific requests for personal information relating to others.

The policy should be read in conjunction with the College’s policy in relation to the handling of requests made under the Freedom of Information Act (FOIA) as there can be considerable overlap between FOIA and the DPA. The principles set out in this policy are also relevant to other related policies (e.g. CCTV, Absence Monitoring, etc.); the relevant data protection issues are set out in the Data Protection Guidelines for Staff that support this policy and in the individual related policies themselves.

4. Responsibilities of Staff

It is a condition of employment that employees should comply with policies and procedures that the College may develop over time. Failure to observe this Data Protection Policy may therefore lead to disciplinary action; serious or deliberate breach of the rules may be regarded as gross misconduct. Breach of this policy may in some circumstances constitute a criminal offence.

All staff therefore need to be familiar with: -

- what personal information they can and cannot collect
- what personal information they can and cannot store
- how and for how long the information should be stored
- what information can and cannot be disclosed
- to whom information can be disclosed and in what format

If there is any doubt as to whether the data should be collected, processed or stored, this should be discussed with the College's data controller.

All staff have a responsibility in relation to the accuracy of information relating to themselves that is held by the College. Staff are required to

- ensure that any information that they provide to the College in connection with their employment is accurate and up to date.
- inform the College of any changes to information, which they have provided, such as changes of address.
- inform the College of any errors in information held about them by the College. The College cannot be held responsible for such errors if it has not been made aware of them by the staff member concerned.

Any member of staff or student who believes that the policy has not been followed in respect of their personal data should firstly raise the matter with the College's designated Data Controller.

5. Responsibilities of Students

As a matter of policy, the College requires all students to consent to the processing of their personal data for educational, administrative and welfare purposes and to comply with this Data Protection Policy. Students are therefore required to familiarise themselves with the content of this policy and with the College's Data Protection Guidelines for Staff, which provides detailed guidance on the application of the Act in specific circumstances.

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that any changes of address are notified to the College via their course tutor.

Students using the College's computer facilities should bear in mind that the Data Protection Act may apply wherever the personal data of other individuals is being

processed. This is particularly likely to arise where information about other individuals is being made available to others on line. This may arise for example, when corresponding via e-mail, internet chat rooms, and when making use of or creating web pages. In cases involving the online publication of personal data relating to other individuals, students should consider seeking the express permission, in writing, of the College's designated data controller before posting online content. Students are similarly required to in mind the data protection principles when processing hard copy personal data such as correspondence and other documents.

Additional guidance on processing personal data can be found in the Data Protection Guidelines for Staff. However, where students are unsure as to whether the processing which they wish to carry out complies with the Act, they should seek guidance from the College's designated Data Controllers before they process the personal data.

6. General Principles for Collecting & Processing Data

The College (including its employees and students) is required by the Data Protection Act to process personal data only where there is a legitimate purpose for doing so, and then only as necessitated by that purpose.

The Data Protection Act doesn't guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals in relation to their personal data and the sometimes competing interests of those with legitimate reasons for using personal information. It applies to all paper records held by the College as well as computer records.

This short checklist will assist those collecting data to ensure that the College complies with the Data Protection Act. Being able to answer 'yes' to every question does not guarantee compliance, and more advice may be required in particular areas, but use of the checklist should limit the risk of breach and help us ensure that we are heading in the right direction.

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm going to be asked to pass on personal information, would the people about whom I hold the information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?
- Have I trained my staff in their duties and responsibilities under the Data Protection Act, and are they putting them into practice?

6.1 Notification

Under the Act, the College is required to notify the Information Commissioner of the purposes for which it intends to process personal data. Notification is a legal requirement and the College is prohibited from processing personal data unless it has notified the Information Commissioner's Office according to its formal procedures. A failure on the part of the College to ensure that its notification is valid and up to date constitutes a criminal offence.

Details of the College's current notification is published on the Data Protection Public Register, a copy of which is at Appendix C.

Updating Notification

- The College shall ensure that its notification is updated annually, **before the expiry of the current notification** as required by the Information Commissioner.
- The College shall ensure that any new, previously unnotified processing, is not carried out until the process of notification has been completed in respect of that data. The College shall carry out regular reviews of the types of personal data which it needs or intends to process, and by whom and how they are to be processed. Staff and students can assist with this process, by informing the College's designated Data Controllers of any new processing which is not covered by the current notification.

Sensitive Personal Data

Sensitive personal data is a special category of personal data. As such it is subject to special protection under the Data Protection Act 1998. Sensitive personal data includes data about:-

- 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

Agreement to the processing of certain personal data (e.g. previous criminal convictions) is a condition of acceptance of a student onto any course, and a condition of employment for staff. .

Therefore, 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. This will include express consent for the types of sensitive information the College has to collect and process. Refusal to sign such a form can result in the offer being withdrawn.

If there is any doubt as to whether the data should be collected, processed or stored, then this should be discussed with the College's Data Controller.

7. How to Obtain Consent

The College should obtain consent to process data, particularly sensitive data, at the point of collection. For example

- student application form
- student enrolment form
- job application form
- contract of employment
- any change of personal details – both staff and student

- student trip information (dietary needs, religious or health reasons)
- sickness information – e.g. return to work form
- questionnaires – student & staff

Consent will be valid only where individuals are provided with sufficient relevant information to enable them to understand what they are agreeing to. They should be provided with any information that would reasonably affect their decision to consent.

Remember that generic consent may not cover certain types of processing, for example disclosure to third parties where this would not be readily anticipated, so that additional specific consent may need to be obtained before personal information can be shared or used in a new way .

In order to ensure compliance with the DPA, and wherever the basis of data collection and use is consent, staff should as a matter of policy, ensure that written records are kept confirming what information was provided as part of the process of obtaining consent and the date upon which consent was granted/withheld

8. Data Controller

The College is a body corporate and is the data controller under the Act, and the Board of Governors is therefore ultimately responsible for compliance with the DPA. However, the College's two designated data controllers will deal with day to day matters.

The College has two designated data controllers: -

- Dave Hibbs – Director of Data College Management - student related data enquiries
- Nicola Perkins – Director of Human Resources – staff related data enquiries

Only these data controllers should access and authorise requests for information

If the information request requires access to network systems (e.g. personal E-mail, personal Z drive) then Computer Services will release the information only upon authorisation from the Director of Human Resources to ensure that management of the data request conforms to the principles of the Data Protection Act. Access to the information will then be under the supervision of the Director of ILT Services to ensure safe, secure and controlled access to the information being requested.

9. General Principles for Data Security

Detailed guidance about the security of personal data can be found in the College's Data Protection Guidelines for Staff, with which staff and students are required to comply. Where staff or students are unsure about any aspect of data security, they should seek guidance from the College's designated Data Controllers

All staff (and students, where applicable) are responsible for ensuring that:

- Any personal data that they hold on behalf of the College is kept securely.
 - Paper records should be stored in a locked drawer or filing cabinet.
 - Information stored on a computer should be password protected
 - Digital & magnetic media used for storage or backup purposes should, be password protected and, where appropriate, encrypted
 - Particular care must be taken in respect of the physical security of portable media (eg disks and data sticks) or laptop computers carrying personal data.
- Personal information is not disclosed in either verbal or written form, deliberately or accidentally to any unauthorised third party.
- Under no circumstances must information be released about an individual to any person requesting this information by phone, fax or post unless the identity of the person making the request and their entitlement to receive the information requested has been confirmed. **Parents (other than in the case of children under 16 who lack capacity to make relevant decisions), spouses, partners, children and employers of students are not entitled to information about another individual – without express consent from the individual concerned**
- Any personal information passed to third parties who process that information on behalf of the College must sign the College's data processing contract. A copy of this contract can be obtained from the College's designated Data Controller.
- Personal data must only be accessed internally by those with a legitimate purpose for doing so and should not be disclosed to external agencies in the absence of proper authority from the individuals concerned or with the approval of the College's Data Controller.
- 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 the processing of personal data takes place should be locked when not occupied. Consideration should be given to door security systems such as key pads in multi-occupied rooms to prevent unauthorised access.
- Staff (and students where applicable) should take particular care with personal data while working remotely – considering particularly:
 - Nature of the data – is it personal? Am I allowed to take it home?
 - Who might be able to see the data – family members; fellow travellers on public transport?
 - Security of the data – both in electronic and paper format

- Physical security of portable media
- Use of password and encryption measures as appropriate

All staff and students are responsible for ensuring that they observe the procedures of the College's IT Acceptable Use Policy and also The Password Policy and Remote Access Policy.

Staff and students should note that unauthorised disclosure of personal data will usually be a disciplinary matter, and may in some cases be regarded as gross misconduct. The individual staff member may also be liable to criminal proceedings.

Staff and students are required to notify the College immediately where they become aware that personal data in their possession has been lost, stolen or damaged so that the College can carry out appropriate risk assessment and take any necessary corrective action in accordance with current Information Commissioner guidance.

10. General Principles of Disclosure

Disclosures will be permitted only where data subjects have **given their consent**, or where the 1998 Act permits transfers without such consent.

The College must ensure that personal data under its control is not disclosed to unauthorised third parties. Unauthorised third parties will include:

- A person or organisation to whom the data subject has not consented that the data be disclosed, unless the 1998 Act expressly permits such transfers without such consent (see below)
- A person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given, unless the 1998 Act expressly permits such transfers without such consent (see below)

"Unauthorised third parties" will include family members, friends, local authorities, government bodies, and the police, unless disclosure without consent is permitted by the 1998 Act (see below), or by other legislation. **There is no general legal requirement to disclose information to the police** although the DPA permits disclosure to the police without consent in certain circumstances. For further guidance, staff should refer to the College's Data Protection Guidelines for Staff.

Consent cannot generally be inferred from silence. Therefore if the College seeks the consent of a data subject in order to respond to a third party request for their personal data, and no response is received from the data subject concerned, the College should conclude that it does not have consent to disclose.

11. Exceptional Circumstances for Disclosure

Data may be disclosed to third parties **without consent**, in some circumstances, for example where it is required for the:

- purpose of protecting the vital interests of the data subject and the data subject is not able to give consent (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
- purpose of preventing serious harm to a third party that would occur if the data were not disclosed
- purpose of safeguarding national security
- prevention or detection of crime
- apprehension or prosecution of offenders
- assessment or collection of any tax or duty or of any imposition of a similar nature
- discharge of regulatory functions, including securing the health, safety and welfare of persons at work

Third parties seeking to access personal data under any of the grounds described above, or any other grounds set out in the Act or in supplementary legislation, should be required:

- to provide reasonable evidence of their personal identity and organisational affiliation according to the circumstances of the request and the nature of the personal data requested

- to conform to any procedural or documentary requirements imposed by the College (i.e. all requests for personal data relating to staff or students be made via the College's Data Controller, and that requests for personal data by police officers should be supported by warrant, or by suitable paperwork provided by the local force stating that the information is required in support of an ongoing investigation) where appropriate, to provide a written and signed document to the College setting out : the purpose for which the data is required; the time for which it is to be held; and an assurance that it will be held and processed in conformity with the Data Protection Principles.

Third party requests for personal data should be passed to the relevant Data Controllers (Dave Hibbs – Director of Data College Management student related data enquiries or Nicola Perkins – Director of Human Resources – staff related data enquiries) who, where appropriate, will authorise the release and format of data.

12.Data 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, should 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.

The College will notify all users, at the point where information is collected from them, the purposes for which the College will be processing the data and any other information necessary to render the collection and processing of data fair.. This notification is known as a "fair processing statement". The consent of the user will be obtained at the point of collection. Data is collected in a range of ways including:-

- Application forms for students
- Enrolment forms
- Telephone enquiries and applications
- Internet enquiries, applications and enrolments
- Application forms for staff
- Application forms for corporation members

All forms used to collect personal data will be reviewed periodically to ensure that they contain an adequate fair processing statement.

The College will ask users to consent to receive promotional campaign 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 and must be given an opportunity to do so.

The College requires students below the age of 18 to consent to disclosure of routine information (e.g. relating to attendance and performance) to parents and guardians (part of enrolment form).

Where students are sponsored by employers to attend College the College will ask students to consent to disclosure of attendance and progress information to employers (part of enrolment form),

Non routine information about students will not be disclosed to parents/employers/other third parties without consent unless the DPA permits such disclosure. It is likely that disclosure without consent will be permitted by the Act only in exceptional circumstances

The College will also ask students if they wish to consent to the Welsh Assembly Government/DCELLS using their data for follow-up activities (part of enrolment form).

Students and staff must ensure that all personal data provided to the College is accurate and up to date. They must ensure that any changes of address are notified to the College via their course tutor. The College will circulate data periodically to data subjects to provide them with the opportunity to update and correct their records.

13. Rights to Access Information

Employees, students, Corporation members and other users of the College have rights to access certain personal data that is being held by the College in relation to them either on computer or in manual files.

All data subjects should be informed that they have the right to access their data. They should be told how they can exercise this right.

The fair processing statement on all College forms will advise data subjects that further information on how to access personal data may be obtained from the Data Protection Officer at Swansea College. This information is also set out in the Student Handbook and the Employee Handbook.

Subject access requests (other than informal routine requests- see section 14 below) received anywhere in the College must be forwarded immediately to the data controller. The data controller will then ask the data subject to complete a Subject Access Request Form (see Appendix B).

The data subject must return the form with 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 includes the personal data of third parties where disclosure would be unfair to the third parties concerned.

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 charge.

On receipt of the Subject Access Request Form and fee the Data Controller will: -

- acknowledge receipt of the request in writing
- notify the subject in writing of the College's intention to comply within 40 calendar days of receipt of the fee and the clearly expressed written request
- Identify the relevant manual and computer filing systems which are likely to contain relevant data
- Consider whether any information should be withheld under the Data Protection Act
- Prepare the information for disclosure

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 which case the data controller will notify the data subject in writing of the reasons for the delay

Manual Unstructured Data

Different rules apply when dealing with subject access requests involving personal data held in manual unstructured records i.e. manual records which are not held in a 'relevant filing system'.

Whilst the procedure for making the request is identical to that outlined above, the College is obliged to comply with a request for manual unstructured personal data only if the time estimate for identifying, locating, retrieving and preparing the data for disclosure does not exceed 18 hours of staff time.

The College is not required, when responding to subject access requests, to provide data subjects with manual unstructured data relating to personnel matters.

14. Responding to "Informal" Requests for Information

Subject to certain exemptions data subjects are entitled to request all the information that the College holds about them. However they are usually looking for something specific. Therefore, the majority of requests received by the College are likely to be from staff and students asking for copies of a specific document(s). These will usually be located in a single source, typically the departmental staff/student files, and will not involve the disclosure of information relating to a third party.

In such cases, whilst the request will technically be a subject access request under the Data Protection Act:

- College policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss.
- Requests should be handled directly by the relevant department or section.
- Take care to ensure that you do not inadvertently release third party information without their consent.
- No fee should be charged.

15. Responding to "Formal" Requests for Information

There may be some instances when a request for information is more complex. It is hoped that such requests will be infrequent.

Examples of situations where more complex requests might arise include:

- request involves locating information from multiple sources
- request involves the release of contentious information
- request is one in a series of requests from the same individual
- request involves the release of third party data for which consent has been refused or cannot be obtained
- the data subject does not want to ask for the information from the department/section that holds it.

In such cases, the request should be referred to the College Data Controller who will ensure that a co-ordinated approach is adopted and will determine whether or not it is appropriate to charge a fee. When responding to formal requests, the Data Controller will liaise with staff in the department/section as appropriate.

The College may also seek legal advice if it is thought that requested information may be exempt under the Act or if disclosure would be unfair to any third party.

16.General Guidance for Requests for Information from Third Parties

Where employment agencies, prospective employers and similar bodies wish to request verification of details about a data subject, such as attendance records, examination results, and degree classifications, the request for the disclosure of the details to the third party should either **come from the data subject directly**, or the request from the third party should be **accompanied by a statement from the data subject** consenting to the disclosure.

Where a request for information is received by **telephone** from an enquirer who appears to be a person to whom information may properly be disclosed, it is good practice to offer to telephone back with the information to ensure some measure of authentication

As an alternative to divulging personal data, the College will be willing to **accept a sealed envelope** which it will attempt to forward to the student's last-recorded address or to forward an incoming email message to a student.

Where the matter is **urgent**, an attempt should be made to contact the student by telephone or other means in order to put him or her in touch with the enquirer

17.Disclosure of Student 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 asked whether they 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. In the absence of consent, student data should not be shared with employers (although where consent is withheld, employers may be entitled to withdraw sponsorship or other support). For further guidance, staff and students should consult the Guidelines for Staff and Students.

18.Students below the Age of 18

Parents and guardians 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 guardians should be considered carefully. It should be normal procedure to request permission from the student before disclosing any additional information.

19. Freedom of Information

It is important to distinguish requests made by individuals for their own personal data, which are covered by this policy, from requests for other information, including requests for third party data, held by the College. The rules governing requests for information held by the College are to be found in the Freedom of Information Act 2000 (FOIA) and the Environmental Information regulations 2004 (EIR). Under FOIA/EIR, information held by the College must be made available to members of the public on request, unless a specific exemption under the legislation applies.

FOIA/EIR and the DPA

Under FOIA/EIR, requests made by individuals for their own data are absolutely exempt as these requests have to be considered under the DPA. Requests made for information about third parties must be considered under FOIA/EIR but this information will be exempt from disclosure under FOIA/EIR if disclosure would breach any of the Data Protection Principles. For example, information would be exempt from disclosure under FOIA/EIR if its disclosure would be manifestly unfair to third party data subjects. Personal information may, however, be provided under FOIA/EIR if no breach of the Data Protection Principles would result. However, as it is not always clear whether a disclosure would breach any of the Data Protection Principles, staff should contact the College's designated Data Controllers wherever requests from members of the public for third party personal data are received.

FOIA Publication Schemes

Under FOIA, the College is also required to routinely publish certain (non-personal) information and further details can be found in the College's Publication Scheme.

Further information about requests for non-personal information can be found in the College's Freedom of Information Act policy, with which staff and students are expected to be familiar, however staff and students should be aware of the following:

- Remember that a request for information, other than the personal data of the requester, is a request under FOIA/EIR **not** DPA
- Where a request asks for both personal information (including third party data) and non-personal information, the request should be broken down and the appropriate parts dealt with under the appropriate Acts (FOIA/EIR and/or DPA). Where staff or students are unsure about the correct way in which to deal with such requests, they should contact the College's designated data controllers
- Where a request asks for environmental information, it should be dealt with under the Environmental Information Regulations 2004 (see College's FOIA policy for further details)
- A request for information does not have to mention the FOIA in order to constitute a valid FOIA request
- Under FOIA/EIR there is no requirement for the requester to provide evidence of his/her identity
- The deadline for complying with FOIA/EIR requests is **20 working days**
- The College may request a fee, based on the administrative cost of complying with the request, or may choose to waive the fee, in accordance with the College's FOIA policy
- Routine information requests for uncontroversial information that is readily available can be dealt with informally.

20. Responsibilities of Contractors and Partners

Data processing terms will be included in all contracts where third parties are involved in processing personal data on behalf of the College and where third parties have access to data as a necessary part of their contracted work.

21. Visitors – including contractors, vendors and suppliers

Certain visitors, including vendors, contractors, and suppliers, are often required to have access to areas in which personal data may be stored or processed. In certain circumstances, it may also be necessary to allow contractors access to personal data (e.g. computer engineers) in the course of maintenance or repair work.

The College should ensure that all visitors (contractors, vendors and suppliers): -

- Report to reception where they sign in and are required to wear some form of identification
- Are escorted throughout the general premises by the person they are visiting
- Are not given unnecessary access to areas where personal data is held or processed
- Are required to sign nondisclosure agreements where access to personal data is unavoidable

22. Transfers of personal data to non-EEA countries

The Data Protection Act 1998 contains specific provisions with regard to the transfer of personal data to countries outside the EEA (the EU Member States, plus Norway, Iceland and Liechtenstein). The eighth data protection principle states "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

The Act sets out a range of circumstances in which data transfers outside the EEA are permissible and it is essential that, where such transfers are to take place, staff are satisfied that they are permitted by the terms of the DPA. Transfers agreed by data subjects will not breach the DPA but consent will be valid only where data subjects are fully informed. When seeking consent to transfer data outside the EEA, data subjects should be made fully aware that countries outside the EEA may not have laws in place to protect personal data. The College will not make such a transfer therefore, without the consent of the data subject unless transfer without consent is permitted under the Act. Consent where necessary should be obtained in writing.

Staff should bear in mind the DPA's restrictions in relation to transfers beyond the EEA when travelling abroad with College laptops and other electronic equipment. Particular care should also be taken when transferring personal data via e-mail and other online communication methods such as the internet, as personal data may inadvertently be transferred outside the EEA in breach of the data protection principles.

23. Medical Information

The College may ask staff and students about particular health needs, such as allergies to particular forms of medication, or other conditions such as asthma or diabetes.

The College will not use or share this information with third parties without explicit consent other than where this is necessary in exceptional circumstances e.g. where required to do so by law or in the interests of an individual's health and safety and where the individual is not capable of giving their consent e.g. in a medical emergency.

24. Standard Student Data Collection & Processing

A large proportion of the personal information with which staff deal on a day to day basis in respect of students will be "standard" i.e. not sensitive information, and will cover categories such as: -

- General personal details such as names and addresses
- Details about class attendance, course work marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

Information about a student's physical or mental health, sexual life, political views, trade union membership or ethnicity or race falls under the category of "sensitive personal information" and is only be collected and processed with the student's consent, other than in exceptional circumstances set out in the DPA.

When collecting, processing and storing any kind of personal information, staff need to ensure that they comply with the Data Protection principles. In particular they must ensure that records are: -

- Collected and used fairly
- Accurate
- Up-to-date
- Stored securely
- Disposed of securely

Staff who are given confidential information by students should not share this information with other staff members unless they have the agreement of the student concerned, other than in exceptional circumstances and with the formal agreement of the College's Data Controller.

Staff Checklist for Recording Students' Personal Data: -

- Do I really need this information about the student?
- Do I know what I'm going to use it for?
- Is the information "standard" or "sensitive"?
- If it is sensitive do I need the student's express consent to process it?
- Does the student know that I've got it, and is he/she likely to understand what it will be used for?
- If I'm asked to pass on the information, would the people about whom I hold the information expect me to do this?
- If I do not have the student's consent to process, am I satisfied that the processing is nevertheless permitted by the DPA?
- Am I sure the personal information is accurate and up to date?
- Have steps been taken to ensure that the data is stored securely?
- Once it is no longer needed, will the personal information be deleted or destroyed?

25. Staff Development on the Data Protection Act and its implications

The College is committed to training all staff on the security procedures required under the 1998 Data Protection Act and raising awareness of the College's guidelines on managing data privacy.

A significant proportion of unauthorised disclosure of, and access to, personal data occurs because employees are unaware of, or fail to follow, existing guidelines.

Swansea College will ensure that when employees are dealing with data, they:

- Are aware what is meant by the term personal data
- Are aware that all personal data – whether held electronically or manually- is subject to the Data Protection Act
- Understand the issues of disposing of paperwork which may hold personal data
- Are aware of the eight principles of data protection and how they apply to their own area of work
- Understand to whom they can disclose personal information and are aware of systems for checking the identity of enquirers
- Are aware who the College designated Data Controllers are
- Formal requests for information should be directed to one of the two designated data controllers
- Are aware of the consequences of unauthorised disclosure – both to the data subject and to themselves

26. Data Security

As a matter of policy, personal data of staff and students should be kept in as few locations as possible e.g. a student file, personnel file, Student Information Directory (SID). Personal information should not be printed off unnecessarily as this increases the likelihood of it being lost or accessed by an unauthorised person. Access should be restricted to those members of staff who have a legitimate reason for accessing it e.g. by using password protection in the case of electronic information, or lockable cupboards in the case of paper information. Further guidance on data security can be found in the Data Protection Guidelines for Staff.

27.Retention of records containing personal 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. Personal records should be retained in accordance with the following guidelines.

Data may be destroyed only with the express permission of the relevant SMT member.

Type of record	Retention period	Reason for length of period
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation.
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985

Health Records	During employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence	Limitation period for negligence.
	At least 10 years for personal and academic references.	Permits institution to provide references for a reasonable length of time.
	Certain personal data may be held in perpetuity.	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.

28. References & Sources

Information Commissioner's Office – Data Protection Act

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

JISC Data Protection Code of Practice for the HE and FE sectors

<http://www.jisclegal.ac.uk/publications/DPACodeofPractice.htm>

-

Definitions of terms in the Act

The following are common terms which are referred to in the Data Protection Act 1998:

Data

Is recorded information that is processed on computer as well as any manual documents held by public authorities.

Processing

Is obtaining, recording, holding, disclosing or doing anything with the data, including disposing of it.

Data Controller

The organisation or person responsible for determining the manner in which and the purposes for which the data is to be used. All references in this policy to the data controller are to Swansea College

Personal data/information

Data that relates to a living individual who can be identified from the information, or could be used with other information we hold, or is likely to be held by us, to identify an individual.

Data Subject

Is the person whose personal information is held by a data controller.

Relevant filing system

A manual filing system organised by reference to individuals or by reference to criteria relating to individuals.

Subject Access Rights

Rights you have as a data subject to ask whether a data controller is holding personal data which relates to you and to be supplied with a copy of it.

Information Commissioner

The Information Commissioner's Office (ICO) is an independent body responsible for ensuring that organisations comply with the Act. It can take enforcement action in cases of breach of the Act and can initiate prosecutions where offences have been committed. The ICO also deals with complaints and enquiries about Data Protection.

Notification

The process by which a data controller notifies the ICO which types of personal information they hold and the purposes for which they process it. These details appear on a public Register of Data Controllers, which anyone can access.

Sensitive Personal Data

Is defined in the Act as data relating to the following:

- Racial or ethnic origin
- Political Opinions
- Religious or other beliefs of a similar nature
- Trade Union Membership
- Physical or mental health or condition
- Sexual Life
- Offences (including alleged offences)
- Criminal proceedings, outcomes and sentences

SUBJECT ACCESS REQUEST

This form is to be completed by an individual who seeks access to personal data held about them by Swansea College.

To help the College comply with your request please give accurate personal details and an indication of the kind of data you are looking for.

Swansea College charges a fee of **£10.00 per subject access request**. The College will try to provide the data you seek within 40 calendar days of receipt of your request, but will contact you if we are not able to meet your request with the target timescale.

Copies of two items of **proof of identity** e.g. birth certificate, passport **must** be included.

SURNAME		FIRST NAME(s)		Date of Birth	GENDER
CURRENT ADDRESS:		ADDRESS: (at time at Swansea College)			
REQUEST: (please indicate)					
STAFF		STUDENT		OTHER	
START DATE	FINISH DATE	SITE/LOCATION		COURSE TITLE/JOB TITLE	
DESCRIPTION OF DATA REQUIRED:					
<p>I enclose a cheque to the value of £10.00 payable to Swansea College.</p> <p>I enclose proof of personal identity.</p> <p>Signed Date</p> <p>Please return this form to the Data Controller, Director of Data College Management, Swansea College, Tycoch Road, Swansea, SA2 9EB</p>					
For Office Use Only					
Date Request Received :			Date of Data Supplied:		
Notes:					

Appendix C



Data Protection Register - Entry Details

Registration Number: Z7502084

Date Registered: 06 February 2003 **Registration Expires:** 05 February 2009

Data Controller: SWANSEA COLLEGE

Address:
TYCOCH ROAD
SKETTY
SWANSEA
SA2 9EB

**This data controller states that it is a public authority under the
Freedom of Information Act 2000 or a Scottish public authority under the
Freedom of Information (Scotland) Act 2002**

**This register entry describes, in very general terms, the personal data being
processed by:**

SWANSEA COLLEGE

This register entry contains personal data held for 8 purpose(s)

Purpose 1

Staff, Agent and Contractor Administration

Data Controllers further description of Purpose:

ADMINISTRATION OF PROSPECTIVE, CURRENT AND PAST EMPLOYEES
INCLUDING SELF EMPLOYED, CONTRACT PERSONNEL, TEMPORARY STAFF
OR VOLUNTARY WORKERS;
ADMINISTRATION OF NON-COLLEGE STAFF CONTRACTED TO PROVIDE
SERVICES ON BEHALF OF THE COLLEGE;
PLANNING AND MANAGEMENT OF DATA CONTROLLERS WORKLOAD OR
BUSINESS ACTIVITY;
OCCUPATIONAL HEALTH SERVICE;
ADMINISTRATION OF AGENTS OR OTHER INTERMEDIARIES;

PENSIONS ADMINISTRATION;
DISCIPLINARY MATTERS, INDUSTRIAL TRIBUNALS ETC.
STAFF TRAINING

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Customers and clients
Suppliers
Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts
Previous and prospective employers of the staff and referees
Agents and contractors

Data classes are:

Personal Details
Family, Lifestyle and Social Circumstances
Education and Training Details
Employment Details
Financial Details
Goods or Services Provided
Racial or Ethnic Origin
Trade Union Membership
Physical or Mental Health or Condition
Offences (Including Alleged Offences)

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

RECIPIENTS OF COLLEGE SERVICES

Data subjects themselves
Relatives, guardians or other persons associated with the data subject
Current, past or prospective employers of the data subject
Healthcare, social and welfare advisers or practitioners
Education, training establishments and examining bodies
Employees and agents of the data controller
Suppliers, providers of goods or services
Financial organisations and advisers
Survey and research organisations
Local Government
Central Government
Courts / Tribunals
Careers service
Trade unions and staff associations

Transfers:

None outside the European Economic Area

Purpose 2

Advertising, Marketing, Public Relations, General Advice Services

Data Controllers further description of Purpose:

THE IDENTIFICATION OF RECIPIENTS FOR COLLEGE SERVICES AND ADMINISTRATION OF PROMOTIONAL CAMPAIGNS;
THE ADVERTISING AND PROMOTION OF THE COLLEGE AND ITS SERVICES INCLUDING BY DIRECT MARKETING MEANS;
THE ADVERTISEMENT AND PROVISION OF GENERAL ADVICE TO MEMBERS OF THE PUBLIC ABOUT COLLEGE SERVICES;
FUNDRAISING FOR THE COLLEGE AND OTHER ORGANISATIONS

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Customers and clients
Complainants, correspondents and enquirers
Relatives, guardians and associates of the data subject
Students and pupils
PERSONS WHO MAY BE THE SUBJECT OF ENQUIRY, PRESS RELEASE OR OTHER PROMOTIONAL EXERCISE.

Data classes are:

Personal Details
Family, Lifestyle and Social Circumstances
Education and Training Details
Employment Details
Physical or Mental Health or Condition

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

RECIPIENTS OF COLLEGE SERVICES
Data subjects themselves
Relatives, guardians or other persons associated with the data subject
Current, past or prospective employers of the data subject
Suppliers, providers of goods or services
Persons making an enquiry or complaint
Trade, employer associations and professional bodies
The media
Trade unions and staff associations

Transfers:

Worldwide

Purpose 3

Accounts & Records

Purpose Description:

Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity

Data Controllers further description of Purpose:

THE ADMINISTRATION OF SUPPLIER RECORDS RELATING TO GOODS, ORDERS, SERVICES AND ACCOUNTS PROVIDED TO THE COLLEGE.

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Suppliers
Students and pupils

Data classes are:

Personal Details
Employment Details
Financial Details
Goods or Services Provided

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

Data subjects themselves
Employees and agents of the data controller
Suppliers, providers of goods or services
Persons making an enquiry or complaint
Financial organisations and advisers
Courts / Tribunals

Transfers:

None outside the European Economic Area

Purpose 4

Education

Purpose Description:

The provision of education or training as a primary function or as a business activity.

Data Controllers further description of Purpose:

ADMINISTRATION OF EDUCATION AND TRAINING (E.G. ADMISSIONS ADMINISTRATION, MONITORING, CALCULATION AND PUBLICATION OF EXAM RESULTS, PROVISION OF REFERENCES);
PROVISION OF EDUCATION AND TRAINING (E.G. PLANNING AND CONTROL OF CURRICULA AND EXAMS, COMMISSIONING, VALIDATING AND PRODUCING EDUCATIONAL MATERIALS, WORK EXPERIENCE PLACEMENTS);

LIAISON WITH EDUCATION, TRAINING ESTABLISHMENTS, EMPLOYERS - PAST, CURRENT AND POTENTIAL;
PREPARATIONS OF DFES RETURNS;
ADMINISTRATION OF STUDENT AWARDS AND FEES (E.G. FREE MEAL ENTITLEMENT, CHARGES FOR EQUIPMENT AND MATERIALS);
ADMINISTRATION OF EXTERNAL VISITS AND RESIDENTIAL COURSES;
ADMINISTRATION OF STUDENT AWARDS AND FEES

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Suppliers
Complainants, correspondents and enquirers
Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts
Students and pupils

Data classes are:

Personal Details
Family, Lifestyle and Social Circumstances
Education and Training Details
Employment Details
Financial Details
Racial or Ethnic Origin
Religious or Other Beliefs Of A Similar Nature
Physical or Mental Health or Condition
Offences (Including Alleged Offences)
STUDENT RECORDS

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

RESIDENTIAL CENTRES, MUSEUMS, THEATRES, LIBRARIES AND OTHER EXTERNAL VENUES FOR VISITS AND COURSES;
UCAS
DEPARTMENT FOR EDUCATION AND SKILLS
Data subjects themselves
Relatives, guardians or other persons associated with the data subject
Current, past or prospective employers of the data subject
Healthcare, social and welfare advisers or practitioners
Education, training establishments and examining bodies
Employees and agents of the data controller
Suppliers, providers of goods or services
Financial organisations and advisers
Survey and research organisations
Police forces
Local Government
Voluntary and charitable organisations
Courts / Tribunals

Transfers:

Worldwide

Purpose 5

Student and Staff Support Services

Data Controllers further description of Purpose:

ADMINISTRATION AND MANAGEMENT OF COLLEGE AND PRIVATELY OWNED PROPERTY (INCLUDING ACCOMMODATION SERVICES);
ADMINISTRATION OF GRANTS AND LOANS (E.G. STUDENT LOANS, LOANS FROM STUDENT LOANS COMPANY, ACCESS LOANS);
ADMINISTRATION AND PROVISION OF LIBRARY SERVICES (INCLUDING MEMBERSHIP RECORDS, LOAN/HIRE RECORDS, INFORMATION AND DATABANK ADMINISTRATION);
TICKET ISSUE/RESERVATION SERVICES;
ADMINISTRATION AND PROVISION OF A STUDENT CARD;
ADMINISTRATION AND PROVISION OF WELFARE AND PASTORAL SERVICES;
CAREERS GUIDANCE;
PROVISION OF CRECHE FACILITIES.

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Suppliers
Relatives, guardians and associates of the data subject
Students and pupils
Business or other contacts
Tenants
WELFARE AND PASTORAL PROFESSIONALS AND ADVISORS

Data classes are:

Personal Details
Family, Lifestyle and Social Circumstances
Education and Training Details
Employment Details
Financial Details
Goods or Services Provided
Racial or Ethnic Origin
Religious or Other Beliefs Of A Similar Nature
Trade Union Membership
Physical or Mental Health or Condition

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

STUDENT LOANS COMPANY LTD
PRISON SERVICE
PROBATION SERVICE
Data subjects themselves
Current, past or prospective employers of the data subject
Education, training establishments and examining bodies
Employees and agents of the data controller
Financial organisations and advisers
Local Government
Courts / Tribunals

Careers service
Trade unions and staff associations

Transfers:

Worldwide

Purpose 6

Crime Prevention and Prosecution of Offenders

Purpose Description:

Crime prevention and detection and the apprehension and prosecution of offenders.

Data Controllers further description of Purpose:

INCLUDES USE OF (THE USE OF CLOSED-CIRCUIT TELEVISION FOR THE MONITORING AND COLLECTION OF SOUND AND/OR VISUAL IMAGES FOR THE PURPOSE OF MAINTAINING THE SECURITY OF PREMISES, FOR PREVENTING CRIME AND FOR INVESTIGATING CRIME.

Data subjects are:

Customers and clients

Offenders and suspected offenders

MEMBERS OF THE PUBLIC THOSE INSIDE, ENTERING OR IN THE IMMEDIATE VICINITY OF THE AREA UNDER SURVEILLANCE.

Data classes are:

Personal Details

Goods or Services Provided

Offences (Including Alleged Offences)

Criminal Proceedings, Outcomes And Sentences.

SOUND AND/OR VISUAL IMAGES

PERSONAL APPEARANCE AND BEHAVIOUR

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

SECURITY ORGANISATIONS

Data subjects themselves

Business associates and other professional advisers

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Police forces

Transfers:

None outside the European Economic Area

Purpose 7

Method 2

Data Controllers further description of Purpose:

PROVISION OF FACILITIES TO OTHER GROUPS OR ORGANISATIONS

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Customers and clients
Suppliers
Advisers, consultants and other professional experts
Students and pupils
Agents and contractors

Data classes are:

Personal Details
Goods or Services Provided

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

Data subjects themselves
Education, training establishments and examining bodies
Suppliers, providers of goods or services

Transfers:

None outside the European Economic Area

Purpose 8

Method 2

Data Controllers further description of Purpose:

PUBLICATION OF THE COLLEGE MAGAZINE

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Students and pupils

Data classes are:

Personal Details
PHOTOGRAPHIC IMAGES;
TEXT OF MAGAZINE ARTICLES

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

STUDENTS AND PUPILS
Data subjects themselves
The media

Transfers:

None outside the European Economic Area

Copyright in this copy is owned by the Information Commissioner. Data Controllers may take copies of their own register entries. Apart from that no part of it may be copied unless allowed under the Copyright Designs and Patent Act 1988.

[© Copyright](#)