

# Data Protection Procedure

## [QP2.28]

|                                    |                                    |
|------------------------------------|------------------------------------|
| Procedure Number:                  | QP2.28                             |
| Revision Number:                   | 3                                  |
| Date of issue:                     | January 2006                       |
| Status:                            | Approved                           |
| Date of approval:                  | May 2006                           |
| Responsibility for procedure:      | Director of Information Management |
| Responsibility for implementation: | Director of Information Management |
| Responsibility for review:         | Director of Information Management |
| Date of last review:               | May 2011                           |
| Date of last revision:             | May 2011                           |
| Date of next review:               | May 2014                           |

## Background

1. Data Protection is an important consideration in the learning environment. Legislation has placed obligations on businesses that process personal data and created rights for people whose personal data is processed. The legislation applies to personal information that is processed by computer and also to personal information held in some types of paper files. This is important to The Adam Smith College, Fife ("the College") because computers, in particular, have now become essential tools in carrying out our work.
2. This Procedure aims to:-
  - Set out practical guidelines on the Data Protection Act 1998 ("the Act");
  - Indicate your responsibilities in relation to the processing of personal data;
  - Prevent unfair or unlawful processing of personal data by, for example, unauthorised retention, disclosure, modification or destruction.
3. This Procedure is a College wide Procedure and indicates how the College will address data protection issues for both students and staff.
4. The College is committed to:
  - protecting personal data of students and staff from unintended loss, destruction, damage, modification, disclosure or other security risk, and
  - to processing personal data of students and staff fairly and lawfully in accordance with current data protection legislation.

## Definitions

5. Data Protection legislation has a language of its own. Some helpful definitions are set out below to assist in your understanding of this Procedure:
  - Data Controller – means a person or company who decides the purposes for which and the way in which personal data is processed. The College is the Data Controller in respect of staff and student personal data.
  - Personal Data – means information about a living person who can be identified by that information or by that information together with other information that the Data Controller has or is likely to obtain.
  - Data Subject – all students and staff of the College are data subjects under the Act.

Other definitions are set out in the body of the text where appropriate.

## Paper Files

6. As previously indicated, the Act applies to personal information held on both computers and in certain paper filing systems.
7. The Act only applies to personal information held on paper records where the paper record is structured by reference to an individual (or by reference to criteria relating to an individual) such that specific information about a particular person is readily accessible. That means that most filing systems will contain personal data. It is only very disorganised filing systems which may fall out-with the Act.
8. It should be assumed, as a general rule, that personnel files and separate files relating to such criteria as disciplinary warnings or appraisals are covered by this Act. However, when in receipt of a subject access request, the College will assess whether or not the information in any particular file is information to which the Act applies before making any disclosure.

## Data Protection Principles

9. All personal data must be processed in accordance with the eight Data Protection Principles. The essence of these principles is set out below at number 10 together with brief, non-exhaustive practical examples of when these principles may have relevance to you.
10. Personal data must:-
  - Be processed fairly and lawfully;
  - Be obtained only for one or more specified or lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
  - Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
  - Be accurate and, where necessary, kept up-to-date;
    - Staff must notify changes of name, address, telephone number, bank and marital status to the HR Department soon as possible. The HR Department will endeavour, periodically, to ask staff to confirm that such personal data held by the College is accurate. Students should advise the College of any changes to their contact details or to any other details that may be of relevance.
  - Not be kept for longer than is necessary
    - As an example, as a student of the College, some parts of your College record may be deleted from computer or destroyed (if manually recorded) at the end of the sixth year following the year in which you

leave the College. The reason that the College retains this information is to assist in establishing facts in the event of a dispute.

- Be processed in accordance with the rights of data subjects.
  - For example, individuals have a right of access to the information that the College holds about them. Upon receipt of a written subject access request and the statutory fee of £10.00 the College shall disclose all the information that it is required to do so by law
  - If any member of staff receives any letter from a customer, business contact, other employee, student or any other third party requesting any information about them then they must pass the letter to the Data Protection Officer, ie the Director of Information Management immediately.
  - Students should, if they are making a subject access request of the College, send their access request to the Director of Information Management.
  - Access to personal data must be restricted to authorised individuals for approved purposes
- Be protected by appropriate technical and organisational measures against unauthorised or unlawful processing, against accidental loss or damage.
  - The College must take steps to put in place technical methods (i.e. firewalls, encryption, password protection, etc.) or organisational methods (hierarchy of access to personnel files, locking cabinets etc.) of protecting personal data where the importance of the personal data makes this appropriate.
  - All students or staff who have access to personal data controlled by the College whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the College, nor any individual employed by the College, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All individuals must fully comply with all College procedures and requirements in this regard.
  - Laptops are particularly vulnerable to theft, especially when used outside of College premises. In these circumstances, staff must keep laptops in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.
  - Personal data should not be stored on laptops unless this is unavoidable and appropriate security measures have been implemented following a risk assessment. This will comprise an encryption and security system. These measures will apply to portable data storage media such as DVDs, mini hard disk drives and USB flash memory data sticks.
  - Personal data must not be transmitted over the Internet unless appropriate encryption methods are used.

- Personal data must not be sent to a third party on portable storage media or in paper form by conventional post. A secure delivery service must be used.
  - Staff should ensure security of employment or student records (whether paper records or computerised) at all times, including out-with the College premises. Staff must not leave personal data on screen or on desk tops when they are not at their desks. Paper records should be stored securely unless under active consideration. A clear desk policy should be observed.
- Not be transferred to a country or territory outside the European Economic Area unless there is a clear legal basis in the Act for making the transfer.

## Statement Detailing The Meaning Of Processing And The Purpose Of Processing

11. Personal data provided by or about an individual to the College will be processed in accordance with the Act. Generally “processing” means using information in any way.
12. Data about an individual will only be processed for lawful and fair purposes. The College is the legal person who determines the manner in which and the purposes for which personal data may be used. The Data Protection Officer who has the main responsibility internally for managing data protection issues and compliance in the College is Director of Information Management.
- The Data Protection Officer is responsible for ensuring the College Data Protection Register entry is kept up to date. It is the responsibility of all staff to inform the Data Protection Officer (via their line manager) of any changes in the type personal data being collected or in the processing of data.
13. Personal data about an individual will be processed for various purposes which may include:

### For Staff

- to assess his/her application to become an employee;
- to administer the contractual sick pay system;
- to address any health and safety issues;
- to facilitate management decisions;
- to detect fraud;
- to administer any personal health insurance benefit or other similar benefit;
- to market College services;
- as part of College tenders or promotions;

- to assist in the administration of claims for grants and other funding;
- to administer an alumni programme; and, generally,
- to administer the employment relationship so that the College may properly carry out its duties, rights and obligations to the employee. Such processing will principally be for HR, administrative, regulatory or payroll purposes;

#### For Students

- to assess any application for enrolment;
- to administer the College/Student relationship;
- to assist in the administration of student loans and other student funding;
- to detect fraud;
- to administer exams or facilitate the certification of exam results;
- to address any health and safety issues;
- to market College services; and, generally,
- to administer the student/college relationship so that the College may properly carry out its duties, rights and obligations in relation
- to ensure equal opportunities
- to claim grant and other funding

There may be other purposes for which your information can be legally used. Where these are non-obvious we will make a note of those purposes available.

## **Sensitive Personal Data**

14. Certain personal data is given special status in data protection legislation. This personal data is called sensitive personal data. Sensitive personal data is personal data consisting of information as to:-
- racial or ethnic origin.
  - political opinions.
  - religious beliefs (or other beliefs of a similar nature).
  - trade union membership
  - physical or mental health
  - sex life
  - commission or the alleged commission of an offence.
  - proceedings for any offence, the disposal of such proceedings or the sentence of any Court in such proceedings.

15. Subject to the exceptions set out below and elsewhere in this procedure, sensitive personal data shall generally only be processed after the employee or student has given express consent. The College may in certain situations process the data without your consent if it is necessary for processing taking place for one of the following purposes:-
- ensuring health and safety of staff;
  - ensuring a safe working environment;
  - maintaining records of statutory sick pay or maternity pay;
  - protecting the person and property of people entering on to the premises of the College;
  - carrying out any other obligation or enforcing any right under employment law.
  - Participating in legal proceedings or obtaining legal advice.
  - For the administration of justice.
  - For medical purposes by a health professional.
16. Sensitive personal data relating to racial or ethnic origin may be processed without express consent in order to monitor the effectiveness of the College's Race Equality Policy and Procedure. The College may also process such sensitive personal data about you without your explicit consent where it is otherwise entitled to do so by virtue of a condition under Schedule 3 to the Act.

## Requests For Information

17. An individual about whom the College holds personal data has the right to be:
- told whether their personal data is being processed by or on behalf of the College and, if so, to be given a description of:
    - i. the personal data held;
    - ii. the purposes for which it is being processed and;
    - iii. the recipients of the personal data
  - given a copy of the personal data in an intelligible format (unless to do so is disproportionate or the person has agreed to an alternative way of providing access)
  - given any information available regarding the source of the personal data
18. The College is entitled to require the individual to pay a fee of up to £10 for any subject access request.
19. Written requests should be directed to the Director of Information Management. If you are a member of staff and you receive a written request then you should forward this to the Director of Information Management immediately.

20. The request for information will be dealt with promptly and in any event within 40 days from the College receiving:
  - the written request for the personal data;
  - sufficient details to allow the College to respond to it;
  - sufficient details to confirm the identity of the person making the request; and
  - a payment of £10.00 where requested.
21. Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained or it is reasonable to proceed without their consent.
22. All requests for access to personal data must be made in writing (which includes e-mails).. You should be aware that where access requests are made via e-mail the fee of £10.00 may still be required and the College need not respond until it is satisfied as to the identity of the individual making the request.
23. Personal information relating to staff and students cannot normally be disclosed to an unauthorised third party. These include family members (see Para 25 below), friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:
  - prevention or detection of a crime
  - apprehension or prosecution of offenders
  - prevention of serious harm to a third party
  - protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
  - ensuring health and safety
24. Staff have the right to expect documentary evidence to support such requests.
25. The Children's Act( Scotland) gives rights to young people when they reach the age of 16, therefore the college is not at liberty to discuss a student with a parent or guardian unless the young person has given permission. Even if permission has been given to staff, caution should be exercised, especially as the person on the phone may not be whom they say they are. If staff are asked to pass messages to a student from a partner, or parent, the best advice is to indicate that a message will be passed on asking the student to make contact with the parent/ partner. This will ensure that hoax messages are not passed on by staff.

## Management Of Personal Data

26. Where we take any decision which significantly affects any member of staff or student exclusively upon the results of an analysis of his/her personal data carried out by automated means then we will provide that person with notice of this fact as soon as reasonably practicable thereafter. If the decision is connected with a contract entered into between the College and an other person or is taken for the purposes of considering whether to enter into or with a view to entering into such a contract, the other person will be allowed to make representations on the outcome of that decision (perhaps as part of a formal grievance procedure).
27. In the event of a potential intended or actual transfer of a business, the College will take all reasonable steps to limit disclosure of personal data about employees to any of the third parties concerned by for instance, the omission of names or other identifying particulars. However, staff should be aware that some personal data such as name, address, position, salary levels may be transferred to a prospective operator (or other similar party) of any part of College operations as part of a due diligence process. Where this happens the College will place contractual obligations on the prospective operator to keep the staff's information safe. The transferee shall cease to be a third party on the date of the formal transfer, except in respect of the personal data concerning certain rights and obligations such as those relating to supplementary pensions – not required under the Transfer of Undertakings (Protection of Employment) Regulations 1981 as amended by the Trade Union Reform and Employment Rights Act 1993.

## Responsibilities

28. We expect all students and staff to use computers, email and the Internet responsibly and in accordance with the data protection principles. You should make yourself aware of the provisions contained in the College's Internet and e-mail Acceptable Use Procedure and Policy.
29. Students and staff are expected to adhere to this procedure and to ensure that those for whom they are responsible both adhere to this policy and protect computer systems and personal data from security risks. Where necessary, managers should seek advice from the IT Department to assist in these goals.
30. Formal responsibility for ensuring that staff and operational procedures comply with the Data Protection Policy and Procedure lies with directors, managers, team leaders or supervisors in each operational area of the College
31. Staff must become familiar with the aims of this procedure and follow the guidelines set out. In particular staff should:

- Seek advice from their line supervisor, team leader, manager or director or the Director of Information Management where they have any doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with the Act;
  - Not use personal information that they hold in the course of their employment for any reason other than the performance of their employment duties. To procure personal information from the College and use it without its consent is likely to constitute a criminal offence under the Act;
  - Provide all assistance to the Director of Information Management in the conduct of any audit or preparing a response to a subject access request;
  - Keep information that you process for the College safe and secure in accordance with any procedures issued by the College. Where no procedures are set out explicitly, you should exercise a degree of care over the personal data that you process by considering the harm that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Director of Information Management.
  - Not keep duplicate records relating to staff or students for the purposes of our employment where a centralised filing option is available. Keeping your own records unnecessarily can complicate the process of responding to subject access requests.
  - Notify the Director of Information Management immediately should you detect any potential or actual breach of the Act.
32. Students must be made aware of the aims of this procedure and follow the guidelines set out. In particular students should:
- Provide all assistance to the Director of Information Management in the conduct of any audit or preparing a response to a subject access request;
  - Speak to the Director of Information Management if they have any questions about this procedure;
  - Not procure personal information from the College and/or use it without its consent. To do so is likely to constitute a criminal offence under the Act.

## Security

33. Any breaches of this Procedure in relation to personal data security will result in disciplinary action and, in serious cases, may result in the dismissal of an employee of the College or the expulsion of a student.
34. Staff and students will be authorised to gain access to certain computer systems, programs and data. No employee or student must attempt, alone or with others, to gain access to data or programs to which they have not been authorised to gain access.

35. Staff and/or Students must not disclose personal details of other staff or students to unauthorised third parties where this information is personal data in respect of which the College is the data controller.
36. The provisions of the Data Security Policy (QP1.44), particularly with regard to the transfer of data to external agencies, must be adhered to.

## **Surveillance At Work**

37. The College has a legitimate interest in monitoring the behaviour of its staff and students that attend the College. For instance, the College may wish to carry out monitoring in order to:
  - Detect harassment or other inappropriate behaviour;
  - Monitor performance of its staff or of students where this is appropriate;
  - Monitor and detect the outward transmission of confidential information;
  - Prevent and detect theft of College property;
  - Prevent or detect any unlawful act;
  - Monitor adherence to this and other policies;
  - Perform other duties in the employment or education sphere.

Monitoring can take several forms. It can involve monitoring by way of Closed Circuit Television (CCTV), e-mail and Internet monitoring or telephone monitoring.

More detailed information about the monitoring of Internet and e-mail activity can be found in the College Acceptable Use Policy.

The College holds information on the destination and duration of calls made from the College telephone system and may use this information if misuse of the system is suspected.

Below, the College sets out its policy with regard to the use of CCTV cameras.

## **CCTV Cameras**

38. In carrying out such monitoring the College may use CCTV cameras in what are considered to be "public" areas of the workplace. Generally, the use of such CCTV cameras shall be notified by using suitable signage at obvious places at the entrance to the monitored areas, however, (even in the absence of such signage) students and staff should be aware that public space within College premises may be monitored in this way. The College has notified such

monitoring to the Information Commissioner and will use the footage in disciplinary or other proceedings where appropriate.

39. The College may also monitor through the use of covert CCTV but it shall only do so where specific criminal activity has been identified. Before starting any use of covert CCTV the College will have made an impact assessment concluding that notifying staff of the use of such covert monitoring would prejudice the investigation and that the use of covert monitoring techniques is a proportionate response to the behaviour in question. Where appropriate, (but at its absolute discretion) the College will involve the police in such monitoring.

## Penalties

40. A failure on the part of the College to comply with the eight Data Protection Principles and the conditions for processing may result in a court order to correct, erase or destroy inaccurate or out of date personal data or to change the way we process personal data. In addition, the court may award compensation arising from a breach of the Act in some circumstances.
41. Use or disclosure of personal data outside the terms notified to the Information Commissioner is a criminal offence, as is the unlawful obtaining or disclosure of personal data. On conviction, both the College and/or individuals responsible may be liable for a fine of up to £5,000.
42. Where an individual suffers damage or loss because of unauthorised disclosure, inaccurate or missing data, or the loss or destruction of data in relation to him/her, he/she may seek compensation from the courts.