Carlisle College

Data Protection Act 1998

Guidelines for staff

Data Protection Act 1998

Guidelines for Staff

Definitions:

Data
Any information which will be or which is being used or processed by a computerised system, or which is recorded with the intention that it will be processed in this way will be “data” for the purpose of the Act.

In addition, any information kept as part of a “relevant filing system” will be data. This may include paper records, or files which are stored alphabetically or another criterion as well as information collected with the intention that it will be filed in such a system. Data can be written information, photographs, or information such as voice recordings or diaries, data sticks and other storage devices.

Personal Data
Information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which the college currently has or may have in the future.

For example, application forms marked only with a number will not identify an individual, but put together with the list of numbers and names, will do so.

Personal data will include names and addresses, features such as hair and eye colour which will often be in the form of photographs, ethnic origin, qualifications and experience, details about sick leave and holidays taken, birthdays or marital status.

Any opinion about intentions regarding a person that are recorded, will also be personal data.

Definitions:

Processing
This covers almost anything which is done with or to the data, including:

- Obtaining the data
- Recording, or entering data onto the files
- Holding data, or keeping it on file, without doing anything to it or with it
- Organising, altering or adapting data in any way
- Retrieving, consulting or otherwise using data
- Disclosing data either by giving it out, by sending it on e-mail, or simply by making it available
- Combining data with other information
- Erasing or destroying data

Data Subject
This is an individual about whom personal data is kept.

Data Protection Act 1998

Definitions:

Sensitive Data
Data is considered sensitive if it is about an individual's racial or ethnic origin, political opinions, religious beliefs, membership, a trade union organisation, physical or mental health, sexual life, offences or alleged offence.

Consent to Process
One of the requirements of fair processing is that the data subject must agree to the processing. Consent requires that there is some active agreement between the two parties.

Processing of Personal Data

All staff will process data about students on a regular basis; when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The college will ensure through enrolment procedures, that all students give their consent for this sort of processing and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

- General personal details such as name and address
- 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 or religious views, trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should seek advice from the Registry Systems Officer.

Before processing any personal data, all staff should consider the following:

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'. If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data? If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?

Processing of Personal Data

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy available on Adminet under Quality policies.

In particular staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept securely and disposed of safely

For further information contact the Registry Systems Officer extension 2786

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 party.

Personal information should be:

- Kept in a secure environment;
- If computerised, password protected;
- If kept on disk or data stick, is itself kept securely.
- Disposed of safely and securely.

Requests for disclosure of personal data

2.1 A disclosure must only take place when any of the following conditions apply:

- When the permission of the Data Subject is given
- Within the college, for authorised functions or registered purposes of the college
- Where the disclosure is by order of a Court

2.2 Disclosing personal data:

- Personal information must not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised party.

The College has a responsibility to ensure that data subjects have appropriate access to details regarding personal information relating to them. Requests should be put in writing to the Registry Systems Officer and may be subject to a charge.

2.3 If common sense suggests that a particular disclosure should be an exception to the rule (eg where someone might be at risk), staff must consult their line manager (as soon as practicable) and make a proper record of the disclosure, to whom it was made and of the circumstances that made the disclosure necessary.

2.4 Where disclosure of sensitive information takes place, a note of the disclosure must be recorded on the appropriate files or case papers.

2.5 Staff must note that the confidential nature of any personal information supplied must be stressed at all times: so they must not take short cuts and always follow the correct procedure.

Refusing to disclose Personal Data

3.1 If you get a call for details about a student (not the student themselves) do not disclose either verbally or in writing. Refer to your line manager or Registry Systems Officer - they can deal with it for you, or advise what to do. Generally ask for all requests to be put in writing

The rule is 'if it doubt, do not disclose"

Disclosure of Personal Data to Prosecuting Agencies

4.1 Section 28 of the Data Protection Act allows for personal data to be disclosed to certain agencies (eg Police, Inland Revenue, Customs and Excise, Public Health Authority, etc) for the purpose of:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty

A disclosure of this kind may be made without fear of making an unauthorised disclosure as long as Data Users can prove that they 'had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters above'.

Disclosure of Personal Data to Prosecuting Agencies

4.2 If staff receive a request for personal data from a police officer, customs official, Department of Social Security and other official bodies, they must ask for the request to be put in writing on official paper, showing the agency crest.

Emergencies

5.1 There may be circumstances where staff have to disclose personal data in emergencies. If an emergency involves a threat to a Data Subject's health or to prevent injury to a Data Subject, then the disclosure can take place.

5.2 A proper record of the disclosure must be made, either at the time, or as soon as possible after the disclosure has occurred. In other urgent situations, staff will have to use their judgement; but in all cases they must keep a formal record of their decision to disclose, and send a note of the disclosure to their line manager.

'Subject Access' to Personal Data

6.1 Staff may be consulted by an individual who wishes to apply formally for Subject Access (ie to access any personal data held by a Data User). If the Data Subject is a student he/she must be referred to the Registry Systems Officer, if the Data Subject is a member of staff to the Personnel Manager. Requests should be put in writing and may be subject to a charge.

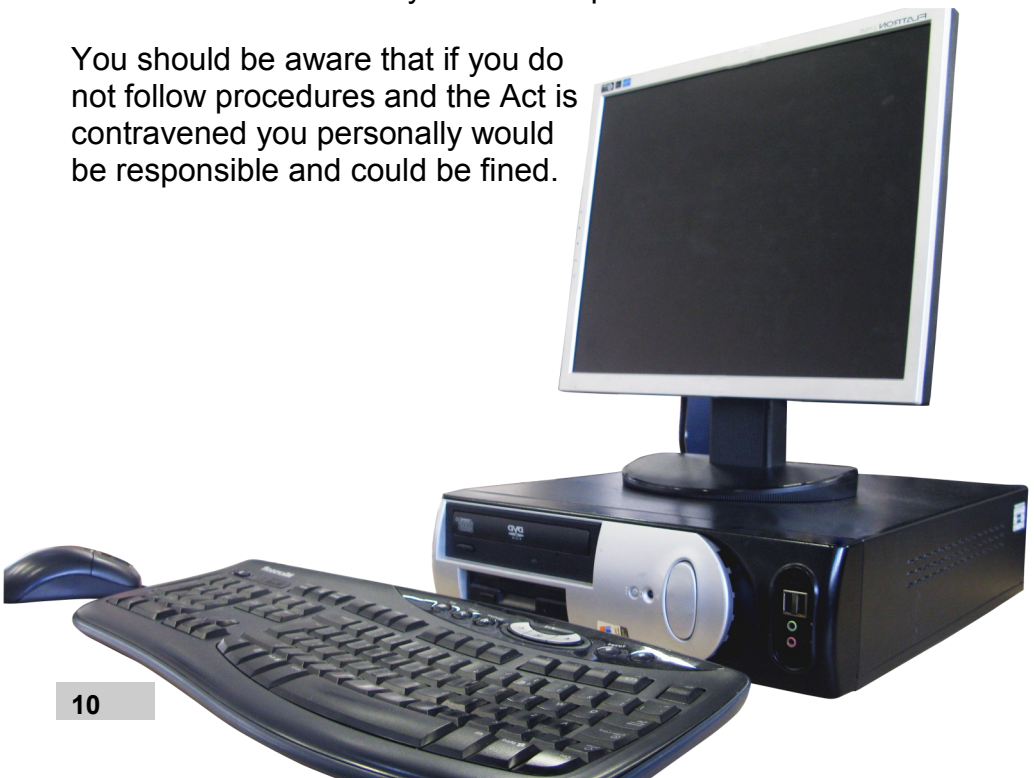
6.2 All staff should be aware that Subject Access is a separate and formal procedure by which personal data are disclosed to the Data Subject.

Personal Data on Home Computers/Laptops

7.1 The Eighth Data Protection Principle states that;
'Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data'.

The college has no control over the security of home computers and laptops or indeed persons accessing them. There is always the possibility of the home being burgled and the computer being stolen, or, if the files are stored on disk, CD or data sticks that these are stolen or lost in transit. The same would apply to paper records (eg contact log). Staff should not normally take home personal information.

You should be aware that if you do not follow procedures and the Act is contravened you personally would be responsible and could be fined.



Professional Opinions

8.1 The Data Protection Act covers any expression of opinion about individuals. As teachers you may routinely record professional opinions. Opinions may be recorded informally in reports, letters, memos etc in a way that is covered by the Act.

8.2 When an opinion is recorded it is good practice to do the following:

- Make it clear that it is an opinion. The record should show who gave the opinion and when.
- If possible provide contact details.
- Structure the record so that if someone objects to its accuracy, his or her view or challenge can be included in such a way that it is given proper weight.

8.3 Ensure that when an opinion is disclosed it is not presented as fact.

8.4 Examples of good and bad practice:

Example	Good practice	Bad practice
A student gets a copy of a report written by his tutor and disputes an opinion recorded in it. He also provides convincing evidence that it includes incorrect factual information	The college explains that it has to be kept as a true record of the tutor's professional opinion but agrees to include the student's comments clearly on his file. The correct factual information is recorded but a record of the error may continue to be held to explain possible unforeseen consequences	The college refuses to record the student's objections to the opinion and only notes the factual inaccuracies

Disposal

Staff must ensure that anything containing personal data is disposed of safely by either shredding or using confidential waste sacks.

Confidential waste collection and disposal can be arranged via the Estate Helpdesk