Data Protection Act (1998)

Main points and considerations

The European Directive 1995— Article 8

"Everyone has the right to respect for his private and family life his home and his correspondence"

"There shall be no interference by a public authority except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others"

The Data Protection Act

The Data Protection Act controls how your personal information is used by organisations, businesses or the government.
Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

The 8 Principles

1) Personal data shall be processed fairly and lawfully
2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3) Personal data shall be adequate, relevant and **not excessive**
4) Personal data shall be accurate and, where necessary, kept up to date
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
7) Appropriate **technical** and **organisational** measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8) Personal data shall not be transferred to a country or territory outside the EU area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Key Definitions:

1) Data Controller - The entity processing / storing data. In our case "the college"

2) Data Processor - Someone who processes data on the Data Controllers behalf, under their instruction. Can be another organisation i.e. sub-contracted provision, WEEE disposal, disposal of confidential paper based documents

3) Data Subject - Any individual; "The person" that data refers to

4) Processing - All that encompasses the processing of data within it's lifecycle:

- Collection
- Input
- Processes, changes, updates etc
- Destruction of ……. You can't pass on the responsibility for destroying data…. We are the Data Controller, responsibility remains with the college!

- What is personal data? **Personal data** means data which relate to a living individual who can be identified –
- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Unauthorised obtaining/disclosing

Caution– this is where we often breach!!

- Paperwork left out on a desk
- Inadvertently passing on personal information over the phone, for example any student information inc attendance to parents of a 18 year old
- Monitor screens displaying personal data i.e. receptions, course advice, enrolment, admin offices, lecturers in class etc
- Allowing others to use your ID / password, do not do it!

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Disclosure to Parents / Guardians

The subject of disclosing data to parents even if the student is under 18 is currently being widely debated in the sector. Currently JISC and most legal organisations are taking the approach that under DPA legislation the data belongs to the subject (the student) and should not be disclosed to a 3rd party (including parents).

Extract from Evershed's
Most parents of children aged under 18 assume that they are entitled to see their child's educational records. However, often institutions have to weigh up whether it is indeed appropriate, particularly where a student lives with only one parent or the student refuses to allow their parents (or one of their parents) to see their records. This can lead to difficult conversations with the student and parents concerned, as it is often unclear exactly whether there is a legal obligation to provide such records.

Extract from JISC Legal guidance;
In general when parents request information (and this may include the "educational record" information where it is not disclosed as above) about their child from a university or college, before responding the institution should consider whether the child, irrespective of their age, **is mature enough to understand their rights. If it is considered that the child can understand their rights, then the institution should respond to the child rather than the parent.**

Data sharing checklist – systematic data sharing:

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.