Data Protection

What is Data Protection?

Data Protection is about protecting individuals’ privacy in relation to the personal data we hold about them. An individual might be a student, an employee, a research participant, contractor, customer or a third party.

Most staff have access to personal data – which might simply be a name and address, the fact that someone’s a student here, a passport photograph or a customer’s details. Personal data is any information which relates to a living individual who can be identified from that data or from any other information in our possession or the public domain.

We might process personal information in a variety of ways, for instance:

- looking at details on a computer
- collecting data as part of a survey, registration process or application form
- holding information in personnel or case files
- storing personal data in an email, committee minute or report
- sharing or distributing individuals’ details

The Act covers personal information whether it is held in paper or electronic records and applies to all personal data processed by the University or those processing such data on its behalf.

The responsibility for ensuring that any personal data we hold on an individual complies with the Data Protection Act rests with ALL of us.

Data Protection Principles

The Act sets out eight key principles. These govern:

- how we gather personal information
- how and where we use it
- who needs to see it
- how we store it and for how long

To apply the principles easily and effectively, we need to be aware of the personal information we are using, the purposes it serves and our grounds for using it.

The principles say that we must:

1. Process personal data fairly and lawfully [This often means having the consent of the data subject or meeting one of the Act's conditions for ‘fair processing’; also making it clear when you are collecting information, how that information will be used and for what purposes].
2. Obtain personal data only for one or more specified and lawful purposes, while ensuring that such data are not processed in a manner which is incompatible with the purpose(s) for which they were obtained.
3. Ensure that personal data are adequate, relevant and not excessive for the purpose(s) for which it is held.
4. Ensure that personal data are accurate and, where necessary, kept up to date.
5. Ensure that personal data are not kept for any longer than is necessary for the purpose for which it was obtained.
6. Process personal data in accordance with the rights of the individuals to whom the information relates.
7. Ensure that personal data are kept secure (i.e. safe from unauthorised access or use, accidental damage or loss).
8. Ensure that personal data are not transferred to a country outside the European Economic Area.
Individuals’ Rights

Under the Act, individuals have the right to know whether the University holds information about them and, if so, what those data are and how they are used. Individuals’ right of access to the information held about them is a means of ensuring that we are complying with the Act and processing their data properly.

When accessing, writing, recording or storing, information on individuals, or accessing their personal data, we should remember data subjects’ right of access and ensure that our actions/statements are defensible. Individuals have the right to object to any processing which causes them damage or distress.

Applications by data subjects to see their data should be forwarded promptly to the University Records Manager, who co-ordinates these requests. Data subjects must pay a standard administration fee of £10 for a request and the University then has 40 calendar days in which to respond.

Sensitive Personal Data

Certain types of personal information are classed as particularly sensitive. For this type of information the data handling rules are even stricter and use of the data will usually require the individual’s explicit consent. Personal data are classed as sensitive where they relate to an individual’s:

- sexuality;
- political affiliation & opinion;
- mental & physical health;
- religious affiliation & beliefs;
- trade union membership;
- race or ethnicity;
- proceedings for, and disposal of, any alleged and/or committed offence;
- actual & alleged criminal acts.

Guidance, Help & Training

The University’s Data Protection Policy and Guidelines can be found on-line at www.york.ac.uk/recordsmanagement/dpa.

The Data Protection website gives further information on the Act and links to other resources. The site also carries information on related pieces of legislation, such as the Freedom of Information Act and Privacy and Electronic Communications Regulations, and relevant policies on the management of records.

The Records Manager can provide further assistance and guidance, and training (see the Data Protection and Professional & Organisational Development websites for training resources and opportunities).

Charles Fonge
University Records Manager and Archivist
Borthwick Institute
University of York

Email: dataprotection@york.ac.uk
Tel: 32(1168)
www: www.york.ac.uk/recordsmanagement

© University of York, 2006