Responsibilities

The Data Protection Act imposes certain responsibilities on students accessing and recording personal data in their studies or other activities.

These obligations include holding and using data in a secure manner, making sure that data is handled in line with what individuals have been told, having appropriate arrangements in place for the access to (and sharing of) data, and making sure that individuals' data is accurate and retained for a suitable period. Most importantly, if a data breach occurs (e.g. personal data held by the student is lost, stolen, inadvertently disclosed to an external party, or accidentally published), this should be reported immediately to the Information Compliance Office so that they may review the circumstances and liaise as necessary with colleagues internally and the relevant external authorities.

1. What is the DPA for?

The Act applies to personal data, held not only in electronic records but also in structured 'manual' (e.g. paper) records. Personal data means data about a living individual who can be identified from the data, or from the data in conjunction with other information (e.g. via code numbers); 'data' includes expressions of opinion about the person. The living individual is referred to as the data subject.

The Act governs the 'processing' of all personal data, which covers almost everything: the obtaining of the data, its retention, its use, and its disclosure, its alteration or destruction.

The Act contains eight data protection principles which apply to all personal data and the processing of it.

Personal data must be processed following these principles so that data are:

1. processed fairly and lawfully and only if certain conditions are met;
2. obtained for specified and lawful purposes;
3. adequate, relevant and not excessive;
4. accurate and where necessary kept up-to-date;
5. not kept for longer than necessary;
6. processed in accordance with an individual's rights;
7. kept in a secure manner;
8. not transferred outside of the EEA without adequate protection.

2. Information which must be supplied to the data subject

When data are collected, the data subject must be told the purpose(s) that their data will be processed for. The data subject should also be told the identity of the data controller and any third parties to which the data will or might be disclosed. This information has to be given at the time of collecting the data or as soon as possible thereafter. Data collected for given purpose(s) can only legitimately be processed for those purpose(s) - not for others of which the data subject has not been informed.

3. When should the data subject's consent for processing be obtained?

If consent is the condition for the processing of personal data, then provision must be made for ceasing the data processing (which includes holding the data) if the consent is withdrawn. Note that the data subject does not have to give a reason for withdrawing consent.

4. Transmission of data to other countries

The Act prevents the transmission of personal data to any country outside the European Economic Area (EEA), unless that country has an adequate level of data protection. However, transfers are allowed where the data subject has given their consent to it, or via the imposition of standard clauses or other EU-sanctioned conditions.

5. Security provisions

All reasonable steps should be taken to ensure that personal data is secure, and the following steps are suggested:

- Access to electronic files and systems should be restricted using privilege levels and passwords.
- Regular password changes should be enforced and the number of attempted logins limited.
- Equipment should be sited in a secure location where access can be restricted to authorised personnel.
- Computers and other devices should be locked when unattended and should be logged-off at the end of a session.
- Redundant data should be wiped or overwritten.
- Appropriate back-up and storage should be observed.
- Portable storage media should be stored carefully.
- Network systems are insecure, and the Cambridge University Data Network is under constant attack from people looking for vulnerabilities. Data must kept as secure as possible, using encryption, de-personalisation and password-protection if possible. Recognised firewalls should be installed.
- Hard copy papers containing personal information should be shredded before disposal; they should not be used as scrap paper.
- Store hard copy files securely. Sensitive personal data should be stored in locked rooms and/or filing cabinets.

6. Security advice on portable equipment

The data controller has a legal obligation under the Data Protection Act to ensure that all personal information is kept secure. This means that information must be protected against unauthorised or unlawful use and against accidental loss, damage or destruction.

Personal information can be held in personal computers, organizers, laptops, tablets, smart phones, paper and other forms. When working away from University premises, information must still be kept secure.

The level of security used to protect information will depend upon an assessment of the security risks. Risk assessment is a consideration of the harm that would result from a security failure (taking into account the potential consequences of a loss of confidentiality, integrity or availability of information) and the realistic likelihood of such a failure. Having considered the risk, appropriate controls can be then be identified and used.

You should consider the following:

- Equipment or media should not be left unattended in public places. If feasible, portable computers should be carried as hand luggage and information carried on separate media from the computer when in transit (e.g. on USB sticks or similar).
- Manufacturer's instructions for protecting equipment should be followed (e.g. protection against exposure to strong electromagnetic fields).

- Computers and other hardware used for processing personal information must have appropriate virus protection.
- Access must be controlled to prevent unauthorised access (e.g. password on start up or secure file encryption).
- Data must be regularly backed up in case of loss or failure.
- All personal data must be removed from equipment before disposal.

Please bear in mind the following technical points:

- Operating system passwords can be bypassed. If the sensitivity of the data merits it, users should consider hard drives with their own password protection or an encrypted file system.
- Leaving wireless access enabled may permit network attacks on laptops, tablets and smartphones.
- Secure deletion means overwriting or reformatting of the media on which the data is stored, not simply pressing 'Delete'.

Technical advice is available from UIS and local Computer Officers.