**UNIVERSITY OF ST ANDREWS**

# DATA PROTECTION POLICY

**[December 2003]**

## I Introduction

1. The University needs to process certain information about its employees, students and other individuals. In so doing, the University is obliged to comply with the provisions of the Data Protection Act 1998. The eight Principles of the Act are described in Appendix A.
2. The Act imposes restrictions on how the University may 'process' personal data. This term covers the collection, recording, retrieval, consultation, use and disclosure of data. Definitions of other terms used in the Act may be found in Appendix B.
3. The University has appointed a Data Protection Co-ordinator to deal with day-to-day Data Protection matters and to encourage good information handling practice within the University.
4. The Act gives to staff and students the right of access [with very limited exemptions] to any personal data the University may hold about them. It also places an obligation on the University to respond to such requests within a set time. For this reason, all formal access requests by staff and students i.e. Subject Access Requests, must be directed through the University's Data Protection Co-ordinator. [See Appendix B for Definition of Data Protection Terms.]
5. The University, all staff and any others who process personal information on behalf of the University, must ensure that they comply with the principles of the Act and with the provisions laid out in 'The Data Protection Act: Staff Guidelines' which may be accessed at http://www.st-andrews.ac.uk/media/staffguide.pdf

## II Status of the Policy

1. This policy has been approved by the University Court. Any breach will be taken seriously, and may result in disciplinary action.
2. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the University. Any failures to follow the policy can therefore result in disciplinary proceedings.
3. Those with honorary contracts or 'visitor' status will also be expected to comply with this policy insofar as they come into contact with personal data through the University.
4. Staff or students who consider that the policy has not been followed in respect of personal data should raise the matter with the University's Data Protection Co-ordinator.

## III The University's Responsibilities

1. The University is committed to protecting the right of individuals to privacy with respect to the processing of their personal data.
2. Under the terms of the Data Protection Act, the University is the Data Controller [see Appendix B for Definition of Data Protection Terms], and ultimate responsibility for compliance with the Act lies with the University Court.
3. Deans, Heads of School/Units and all in managerial or supervisory roles have a responsibility to ensure good information handling practice amongst all members of the University.

## IV Staff Responsibilities

1. When processing personal data about students or colleagues, staff must comply with the Staff Guidelines as described above.
2. Staff are responsible for the security of the data they process, and for ensuring that it is not disclosed to anyone who is not entitled to it.
3. Staff are also Data Subjects [see Appendix B for Definition of Data Protection Terms]. They should ensure, therefore, that any information they supply to the University in connection with their employment is accurate and up to date. The University cannot be held accountable for errors arising from changes about which it has not been informed.

## V Right of Access

1. Staff, students and other users of the University have the right to access personal data held about them by the University, whether in manual or electronic format.
2. Any individual wishing to exercise this right should apply using the Subject Access Request form available from the Data Protection Co-ordinator.
3. The University will charge £10 per request.

## VI Information and Guidance

Further information on the application of the policy and practice may be obtained from the University's Data Protection Co-ordinator.

# DATA PROTECTION POLICY APPENDIX A

## Principles of Data Protection

Anyone processing personal data must comply with the eight enforceable principles of good practice. These say that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the Data Subject's rights
- secure
- not transferred to countries without adequate protection.

### Fair and lawful

The intention of the Act is not to prevent data processing, but to ensure that it is done fairly and without adverse effect on the individual the data relates to. The Data Subject should be informed of who the Data Controller is [in this case, the University]; who the Data Controller's representative is [in this case, the Data Protection Co-ordinator]; the purpose or purposes for which the data are to be processed; and to whom the data may be disclosed. For students this will be done as part of the matriculation process. Personal data processing may only take place if specific conditions have been met – these include the Data Subject's having given consent or the processing being necessary for the legitimate interests of the Data Controller. When it comes to processing sensitive personal data [data relating to ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject] additional conditions must be met - in most cases this will require explicit [ie written] consent from the individual concerned.

### Purposes

Personal data processing must be in accordance with the purposes notified by the University to the Data Protection Commissioner – in other words, you cannot gather information for one declared purpose, and then use it for another. If any 'new processing' is to take place the Data Protection Co-ordinator must be consulted.

### Adequate, accurate, timely

The fact that electronic information is readily available does not mean that it can be treated casually. Nor can it be gathered and held because it might be useful some day, or simply because the software allows it. The requirement that personal data should not be kept

longer than is necessary means that a policy should be in place for the disposal of the data once it has reached the end of its life - there can be no holding on to data simply because it is easier to do so than to ensure its disposal.

**Data Subject's rights**

The data must also be treated with regard to the Data Subject's rights, such as the right to have inaccurate data amended. A Data Subject has the right to request access to any data held about him or her within the University systems - consequently, the University must make provision to ensure that that data is retrievable from its systems.

**Security**

Appropriate security measures must be taken against unlawful or unauthorised processing [including unauthorised viewing] of personal data and against accidental loss of, or damage to, personal data. A Data Subject may apply to the Courts for compensation if he or she has suffered damage from such a loss. The Act puts HE institutions under an obligation to have in place policies, procedures and technologies to maintain the security of all personal data from collection to destruction. This covers not only the storage, but also the transmission, of personal data [including email.]

**Transfer of personal data**

Personal data must not be transferred to a country outside the European Economic Area unless specific exemptions apply (e.g. if the Data Subject has given consent.) This includes the publication of personal data on the internet.

# DATA PROTECTION POLICY APPENDIX B

## Definition of Data Protection Terms **Data**

Data means information:

- stored in a form capable of being processed by computer [such as word-processed documents, spreadsheets and databases]
- recorded in any form for later processing [such as registration forms, CCTV pictures]
- stored as part of a 'relevant filing system'. Note that this definition is very broad and covers such things as card indexes and microfiche files as well as traditional paper- based files. It would be as well to assume that any paper-based data falls under the Act.

### Personal Data

Personal data are defined as data which relate to a living individual who can be identified:

- from those data; or
- from those data and other information in the possession of [or likely to come into the possession of] the Data Controller
- and includes any expression of opinion about the individual and any indications of the intentions of the Data Controller or any other person in respect of that individual.

The Information Commissioner [previously the Data Protection Commissioner] accepts that this definition is 'not without difficulty'. It would always be safest to assume that data is personal rather than not.

### Sensitive personal data

The 1998 Act distinguishes between ordinary "personal data" such as name, address and telephone number and "sensitive personal data" which includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive personal data is subject to much stricter conditions.

**Data Subject**

A Data Subject is any living person who is the subject of personal data.

**Data Subject Access**

This is the right of an individual to see personal data relating to him or her which is held by a Data Controller.

**Data Controller**

A 'Data Controller' is any person who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place. The University is the Data Controller, but any member of staff may also be a Data Controller if he or she makes decisions about personal data and its processing.

**Processing**

Processing covers almost anything you can do with data, and includes acquiring, recording, consulting, retrieving, and making the data available to others.