KINGSTON UNIVERSITY

CONFIDENTIALITY – DATA PROTECTION ACT 1998

The Data Protection Act 1998 is concerned with the protection of human rights in relation to personal data. The aim of the Act is to ensure that personal data is used fairly and lawfully and that, where necessary, the privacy of individuals is respected.

The definition of personal data includes all data which relates to a living individual who can be identified, either from the data, or from the data and other information which is held by the same person as the data. Unlike the 1984 Act, which only covered data held on computers, the 1998 Act covers all forms of data whatever the media on which it is held. So paper files, card indexes and computer data are all covered.

Most University staff will have some contact with personal data and it is therefore essential that they should be aware of the main provisions of the Act. In some circumstances individual members of staff can be held personally liable for breaches of the Act.

DATA PROTECTION PRINCIPLES

Under the Act all users of personal data must comply with a number of data protection principles. These state that personal data must:

- be processed fairly and lawfully
- be obtained only for one or more specified and lawful purposes and must not be used in any manner incompatible with that purpose or purposes
- be adequate, relevant and not excessive for the purpose or purposes
- be accurate, and where necessary, kept up to date
- not be kept for longer than necessary for the purpose(s) for which it was obtained
- be processed in accordance with the rights of the person it concerns
- be protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, or destruction or damage
- not be transferred to a country outside of the European Economic Area unless that country has an adequate level of protection for the rights and freedoms of the individual similar to the Act itself.

CONDITIONS FOR PROCESSING

In addition to the principles it is necessary to meet various conditions for processing. Ideally the consent of the individual should be obtained before data about them is processed. However, this is not always possible and so the Act does permit other conditions to be met in order for processing to take place. It should be noted that processing includes just storing personal data.

When supplying data people should be told the purposes for which it will be used. They must

also be told if any data will be supplied to a third party (ie. to anyone outside of the University).

SENSITIVE DATA

The Act defines certain types of data as "sensitive data". All data relating to the following is regarded as sensitive:

- racial or ethnic origin
- political opinions
- religious beliefs or other similar type beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- criminal record and details of any proceedings for offences including the sentence.

Any member of staff who processes sensitive data must meet more stringent conditions under the Act and must normally have the *explicit* consent of the person, about whom data is held, to process that data. Use of data for ethnic monitoring is permitted.

YOUR RESPONSIBILITIES

All staff are required to maintain confidentiality in their work as appropriate. In relation to personal data it is essential to review procedures for handling such data to ensure that all processing is lawful under the Data Protection Act, 1998. These points should be particularly considered:

- Access to personal data should be restricted to those who need it for clearly defined purposes. Personal data held on computer should be protected by regularly changed passwords, while data held on other media should be kept secure when not in use. Action should be taken promptly to investigate and remedy any security breaches. Failure to protect against unauthorised access would be an offence under the Act.

- Data must only be used for purposes for which it is collected and so data collected for one purpose must not be used for other purposes unless these were made known at the time the data was collected, or the data subject is advised and consents.

- Data should not be held for longer than necessary and so should be destroyed when no longer needed, or at the end of any statutory retention period. Only keep data if there is a good reason for doing so – getting rid of unnecessary data could save space!

- Take care when revealing personal data to anyone other than the person themself. Especially take care when revealing data to students or members of the public. Where necessary obtain evidence of identity and establish why the data is needed. Consider whether or not revealing the data is in accordance with the Act and, if in doubt, seek advice. The consent of the Data Subject should be obtained whenever possible.
- Requests from individuals to be removed from direct marketing mailing lists must be complied with.

- If in doubt about a particular action it is worth considering how one would feel if one's own data was to be used in a particular way. Remember the human rights basis of the Act. If in doubt, seek advice from the University Data Protection Officer.

NOTIFICATION

The University is required to Notify the Information Commissioner of the ways in which it processes personal data and of the types of data held. If you are establishing a new system of processing please check with the University Data Protection Officer to ensure that such processing is either covered by the existing notification or that an amendment is submitted.

LIABILITY

You are, of course, expected to maintain high standards in your work. There is an agreed Disciplinary Procedure which is used to deal with proven cases of incompetence or negligence. Kingston University will not, however, take legal action against its staff and will indemnify individual staff against legal action by others, provided staff concerned have not been guilty of fraud, gross misconduct, or any criminal offence.

This applies to the Data Protection Act as well as to other aspects of your work. However, you should be aware that certain breaches of the Data Protection Act by individual staff may be criminal offences.

THE RIGHTS OF INDIVIDUALS

The Data Protection Act, 1998 gives individuals certain rights to know what data is held about them and what it is to be used for. There are some transitional exemptions for non-computerised records (eg. paper) but, in principle, anyone has the right to see copies of all data held about them on any media. A charge of up to £10 may be levied for such access. There is also a right to have any inaccuracies in data corrected or erased.

Individuals also have the right to request that their data not be used for direct marketing purposes. Such requests must be made in writing and only relate to marketing specifically addressed to individuals.

Any request for access to data under the Data Protection Act should be immediately referred to the University Data Protection Officer. There are strict time limits on the provision of access and therefore any delay may put the University at risk of breaching the Act.

ENQUIRIES

Any questions relating to the Data Protection Act should be addressed to the University Data Protection Officer, River House.

Any staff processing, or proposing to process, sensitive data or who may be sending any data overseas outside of the European Union, are advised to discuss the matter with the Data

Protection Officer.