Document Title		
Data Protection Policy		
Document Author and Department:	**Responsible person and Department:**	
David Farley, Data Protection Officer, Library	David Farley, Data Protection Officer, Library	
Approving Body:	**Date of Approval:**	
Board of Governors – policy Planning and Resources – guidelines and forms	16 March 2011 1 February 2011, 12 November 2013	
Date coming into force:	**Review Date:**	**Edition No:**
16 March 2011	**March 2016**	**2**
EITHER **For public access?** Tick as appropriate	**OR** **For internal access only?** Tick as appropriate	
YES ✓	**YES**	
Applicable to collaborative provision? Tick as appropriate		
YES	**NO** ✓	
Summary/Description:		
The Data Protection Policy ensures the University's compliance with the Data Protection Act 1998. This edition replaces the previous Policywhich was approved in 2004. Minor modification in 2013		

THE UNIVERSITY OF WINCHESTER

Approved by Board of Governors on 16 March 2011
Modified by Planning & Resources Committee 12 November 2013

THE DATA PROTECTION ACT 1998

DATA PROTECTION POLICY

The Data Protection Act 1998 places obligations on the University and its employees. To comply with the Act, personal data must be collected and used fairly, stored and disposed of securely and not disclosed to any unauthorised person.

1 Definitions

“University Data Protection Officer” is the person designated by the University as its representative under the Act – currently the Librarian.

"Data controller" is any person who makes decisions with regard to particular personal data, including decisions about the purposes for which the personal data are processed and the way in which the personal data are processed.

"Data subject" is an identifiable or identified living individual who is the subject of personal data.

"Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

"Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.

"Sensitive personal data": The 1998 Act distinguishes between "ordinary personal data" such as name, address and telephone number and "sensitive personal data" including 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 such data is subject to much stricter conditions.

"processing" is the obtaining, recording or holding information or data or carrying out any operation or set of operations on information or data, including; organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or; alignment, combination, blocking, erasure or destruction of the information or data;

A “data user” is any member of the University who records, and/or processes personal data in any form.

2. Introduction

The University of Winchester is a data controller under the Data Protection Act 1998. The information and guidelines contained within this policy and its accompanying guidance apply to the whole University community, both staff and students.

Like all educational establishments, the University holds and processes information (personal data) about its employees, applicants, students, alumni and other individuals (data subjects) for a variety of proposes such as the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll, and to enable correspondence and communications.

To comply with the Data Protection Act 1998, personal data must be collected and used fairly, stored and disposed of securely and not disclosed to any unauthorised person. The University also has an obligation as a data controller to notify the Information Commissioner of the purposes for which it processes personal data. Full details of the University’s data protection registration with the Information Commissioner are available from the Data Protection Officer, or from the Information Commissioner’s website <http://www.dataprotection.gov.uk/>.

The University policy has been prepared in accordance with the British Standards Institute *DISC Guide to the Implementation of the Data Protection Act*; and the Joint Information Systems Committee *Data Protection Code of Practice*.

3. The 1998 Act

3.1 Aims

There are three basic tenets underlying the 1998 Act: purpose, fairness and transparency.

Purpose

Data controllers are required by the 1998 Act to process personal data only where they have a clear purpose for doing so, and then only as necessitated by that purpose. A data controller's purpose for any personal data processing operation should thus be clearly set out in advance of the processing, and should be readily demonstrable to data subjects.

Fairness

Both the 1998 Act and the Information Commissioner recognise that there are many legitimate purposes for the processing of personal data, even where data subjects may not wish this to happen. The essential element here is that of ensuring fairness in the relationship between data controller and data subject. Thus, where a data controller has identified a particular purpose for processing of personal data, they must also consider its fairness. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation. For many others, data controllers will need to make their own determination as to the requirements that will have to be met for processing to be deemed fair.

Transparency

It is clear from the 1998 Act that much of the onus for ensuring effective enforcement of their rights will lie with the data subject. The 1998 Act requires data controllers to provide data subjects with a basic minimum amount of information about the collection, use, and distribution of their personal data. Data subjects therefore need to know the purpose of the processing, and the measures that the data controller has taken to ensure that the processing is fair.

3.2 The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
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 in relation to the purpose or purposes for which they are processed.
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 the 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 EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.3 Data Subject Rights

The Act gives rights to individuals in respect of personal data held about them by data controllers. These include the rights:

- To make subject access requests about the nature of the information and to discover to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for the purposes of direct marketing
- To be informed about the mechanics of any automated decision-taking process that will significantly affect them
- Not to have significant decisions that affect them made solely by an automated decision-taking process

- To take action for compensation if they suffer damage by any contravention of the Act by the data controller
- To take action to rectify, block, erase or destroy inaccurate data
- To request the Information Commissioner to make an assessment as to whether any provision of the Act has been contravened

4. Compliance with the policy

Compliance with the 1998 Act is the responsibility of all employees and students of the University. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, access to University facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the University Data Protection Officer.

4.1 Responsibilities of all data users

4.1.1 Lawful processing

All personal data processing undertaken by data users in the course of their employment by the University must be in compliance with the Data Protection principles. In particular, personal data processed by University employees shall:

- be kept up to date and accurate as far as is reasonable
- not be processed without the data subject's consent (see section 4 below)
- not be used for purposes other than that for which it was collected
- be kept for no longer than it is required for the purpose for which it was originally collected.

4.1.2 Retention of personal data

Despite the general requirement that data not be kept longer than is required for its declared purpose, the 1998 Act does permit the retention of records for research and archival purposes. The Librarian is responsible for the selection and preservation of University records and for making them available for administrative and research purposes.

4.1.3 New or additional processing

No employee of the University may, without the prior written authorisation of the University Data Protection Officer:

- Develop a new computer system for processing personal data
- Use an existing computer system to process personal data for a new purpose
- Create a new manual filing system containing personal data
- Use an existing manual filing system containing personal data for a new purpose

4.1.4 Data Security

All employees of the University are responsible for ensuring that:

- Any personal data, which they hold or process, is kept securely
- Personal data is not disclosed orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort is made to see that personal data is not disclosed accidentally
- All third party requests for access to personal data, including those from the police, are directed to the University Data Protection Officer.

Unauthorised disclosure is a disciplinary matter. If in any doubt consult the Data Protection Officer.

Further guidance is available on the University website.

4.2 Additional Responsibilities of Deans of Faculties and Directors of Professional Services

In addition to their responsibilities as data users, Deans of Faculties and Directors of Professional Services have additional responsibilities regarding the operation of this policy, which are:

- Informing the University Data Protection Officer of processing of personal data within the University that may need to be notified to the Information Commissioner
- Gaining the consent of data subjects for the processing of personal data held on them by the University
- Providing personal data to the University Data Protection Officer in response to a subject access request when requested to do so by the University Data Protection Officer, and
- Maintaining the security of, and access to, personal data within their Faculty/Department.

4.3 Responsibilities of Applicants and Students

Applicants and students must ensure that any personal data supplied to the University is accurate and up-to-date. They must ensure that any changes of address or other personal details are notified to Registry in the case of applicants or to Student Services in the case of students. Students using University computing facilities are required to comply with the data protection provisions of the University ITS Regulations. Students involved in organising clubs and societies are also obliged to comply with the Act.

4.4 Responsibilities of employees

All employees must ensure that any personal data supplied to the University is accurate and up-to-date; and that the University is informed of any errors in, or changes to, information which they have provided, e.g. changes of address or marital status.

5. Consent to Process

It is the University's policy to seek consent whenever practicable from individual data subjects for the main ways in which the University may hold and process personal data concerning them. Although many types of personal data may, at the discretion of the University, be fairly and lawfully processed by the University under the 1998 Act without the need to obtain data subjects' consent, the obtaining of consent is the simplest way of ensuring that all parties are aware of their rights and obligations under the Act. This also allows individuals to raise any objection to the intended processing of their personal data. The University will consider any objections, but reserves the right to process personal data in the absence of consent, where such processing is permitted by reason of fulfilling one of the criteria within Schedule 2 of the Data Protection Act, for example, where the University needs to process personal data to carry out legitimate University functions, or in order to comply with a legal obligation.

All current and prospective employees, admissions applicants, and students will be asked to sign a consent form regarding particular types of information which the University may in due course hold and process concerning them.

6. Sensitive Personal Data

The University may from time to time process sensitive personal data relating to admissions applicants, students and employees of the University.

The University will normally only hold or process sensitive personal data with the explicit consent of the data subject, but reserves the right to process sensitive personal data in the absence of explicit consent, where such processing is permitted by reason of fulfilling one of the criteria within Schedule 2 and one of the criteria within Schedule 3 of the Data Protection Act, for example, to perform a legal duty regarding employees, or to protect the data subject's, or a third party's, vital interests.

7. Disclosure outside of the EEA

The University may, from time to time, wish to transfer personal data to countries or territories outside the European Economic Area in accordance with purposes made known to individual data subjects. Other personal data, even if it would otherwise constitute fair processing, will not, unless certain exemptions apply or protective measures are taken, be disclosed or transferred outside the EEA to a country or territory that does not ensure an adequate level of protection for the rights and freedoms of data subjects. The EEA does not include the Channel Islands or the Isle of Man. This Section is subject to exclusions of certain data as outlined in Section 8

8. Public Display of Employee Data

In order to assist with the proper functioning of the University, the University may provide or publish employees' University telephone number, University address, e-mail address, photograph and appropriate information about their University duties, whether in hard copy and electronic directories, upon enquiry, or on such websites as are approved by the University from time to time. Any objection to the provision of such details by the University in such circumstances should be provided to the Librarian in writing for consideration.

9. Closed Circuit Television

The University uses Closed-Circuit Television as part of its security system. This will be done within the CCTV Data Protection Code of Practice, issued by the Information Commissioner in July, 2002

10. Subject Access Requests

An individual who wishes to exercise their right of subject access with regard to the University is required to complete the University Subject Access Request Form and to submit it to the University Data Protection Officer. Copies of the form and an explanatory leaflet are available from the University Data Protection Officer and on the Portal. The University will make a charge of £10 (or other such charge as may be permitted by secondary legislation under the 1998 Act) on each occasion that subject access is requested, and this fee must accompany the University Subject Access Request Form. In accordance with the 1998 Act, the University reserves the right to reject repeated requests where a reasonable period has not elapsed between requests.

On receipt of a completed University Subject Access Request Form (including adequate evidence of the data subject's identity) and payment of the required fee, the University shall respond within 40 days. The information that the University will supply will include an explanation of any codes contained within it. The data supplied will, in principle, be all that held at the time that the request is made, although the law permits routine amendments and deletions of data to continue between the time of the request and the time of the reply, and to this extent the data supplied may differ from that held at the time the request was made, although no special amendments or deletions will be made.

If the data subject has reason to believe that the University has not dealt correctly with their access request, the matter should be taken up in the first instance with the University Data Protection Officer. If the data subject remains unsatisfied after discussion with the University Data Protection Officer, they should raise a complaint under the University's Complaints Policy. If they remain unsatisfied they should then contact the Information Commissioner who is officially appointed to consider such complaints. The address is: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Approved by Planning and Resources Committee on 1 February 2011

THE DATA PROTECTION ACT 1998

DATA PROTECTION GUIDELINES: STAFF

Introduction

The Data Protection Act 1998 governs the ways in which data relating to individuals may be processed. Many of the day to day activities carried out by staff of the University as part of their academic, administrative, or service work will involve the processing of information relating to identifiable living individuals. Staff should be aware that processing of such information, which may be held in any office, or by any staff member, of the University constitutes 'personal data processing' and is subject to the provisions of the Data Protection Act 1998, including the eight Data Protection Principles noted below.

All personal data collected, held, and processed, via automatic means, including WWW tools and other Internet software, are thus subject to the Data Protection Principles, as are all personal data contained in structured manual files.

The University expects its members not only to comply with the legislation but to safeguard personal information in accordance with best practice in the light of the principles of data protection. These Guidelines summarise the implications of data protection legislation for the University and provide a set of guidelines that deal with individual points in more detail. Members of the University who are unclear about the data protection implications of any aspect of their work should seek the advice of the University Data Protection Officer.

The University was registered under the Data Protection Act 1984. This registration will be continued in an appropriate form under the Data Protection Act 1998. The registration may be accessed via the web pages of the Office of the Information Commissioner or on application to the University Data Protection Officer. The University has a Data Protection Policy, which is available for consultation on the Portal.

Definitions

"Personal data" - "Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.

"Sensitive personal data" - The 1998 Act distinguishes between "ordinary personal data" such as name, address and telephone number and "sensitive personal data" including 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 such data is subject to much stricter conditions.

"Processing" – the obtaining, recording or holding information or data or carrying out any operation or set of operations on information or data, including; organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or; alignment, combination, blocking, erasure or destruction of the information or data;

"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 personal data are processed and the way in which the personal data are processed.

"Data subject" - A "data subject" is an identifiable or identified living individual who is the subject of personal data.

"Data subject access"- "Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
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 in relation to the purpose or purposes for which they are processed.
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 EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Your Rights

You are entitled to have access to information held about you by the University, except where releasing that information would breach another person's privacy, and subject to other exemptions contained in the 1998 Act. You also have rights including rights to

- prevent processing likely to cause damage or distress;
- prevent processing for the purposes of direct marketing;
- request that inaccurate data held on you by the University, and any other personal data in respect of which the University is the data controller and which contain an expression of opinion which appears to be based on the inaccurate data, is rectified, blocked, erased or destroyed.

It is the University's policy to seek consent whenever practicable from individual data subjects for the main ways in which the University may hold and process personal data concerning them. Although many types of personal data may, at the discretion of the University, be fairly and lawfully processed by the University under the 1998 Act without the need to obtain data subjects' consent, the obtaining of consent is the simplest way of ensuring that all parties are aware of their rights and obligations under the Act. This also allows individuals to raise any objection to the intended processing of their personal data. The University will consider any objections, but reserves the right to process personal data in the absence of consent, where such processing is permitted by reason of fulfilling one of the criteria within Schedule 2 of the Data Protection Act, for example, where the University needs to process personal data to carry out legitimate University functions, or in order to comply with a legal obligation. You will be asked to sign a consent form that will identify the personal information the University will hold on you in support of its general business functions.

Subject Access Requests

As a matter of policy, the University will normally make certain parts of the personal data held on you accessible on request. This data includes:

Name
Address
Post title
Salary point and grade
Next of kin
Qualifications

However, under the 1998 Act you are also entitled to make what is know as a "subject access request" to access and obtain in permanent form a copy of any personal data held on you by the University that is not subject to exemption by the Act. If you wish to make a subject access request, your request must be:

- made in writing (this may be in electronic form)
- accompanied by a fee of £10

Before we can act on your request, we must:

- be sure of your identity
- be supplied with information from you in order to locate the information you seek

You are entitled:

- to be informed whether your personal data are being processed by the University
- to have the information constituting the personal data communicated to you

You may apply to access your data in writing in any way you choose. A Subject Access Request Form and Guidance document is available from the University Data Protection Officer for your convenience.

On receipt of your completed request and payment of the fee, the University is obliged to respond in 40 days. This period may be extended if we need further information from you. The information that we give to you will include an explanation of any codes contained in it. The data will be in its latest form.

If you have any reason to believe that the University has not dealt correctly with your request, please first take the matter up with the University Data Protection Officer. If you remain unsatisfied after discussion with the University Data Protection Officer, you should raise a complaint under the University's Complaints Policy. If you remain unsatisfied you should then contact the Information Commissioner who is officially appointed to consider such complaints. Her address is: Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Your Responsibilities

Any collection, processing, or retention of personal data carried out by you as part of your academic, administrative, or service work for the University must be carried out in accordance with the Data Protection Principles.

Where you process personal data for which the University is Data Controller, as a legitimate part of your employment (e.g. research, teaching, consultancy and administration), you may usually rely upon the notification to the Information Commissioner provided by the University. It is, however, important that you inform the University Data Protection Officer of any new purposes for which you intend to process personal data before you begin that processing, and that you ensure that your processing remains, at all times, in compliance with the 1998 Act. Breaches of the Act in the course of your employment could open the University to legal action by data subjects, and may thus lead to disciplinary action against you by the University.

If you process personal data for which the University is not Data Controller, e.g. processing for the purposes unrelated to your University employment, this processing may require a personal notification to the Information Commissioner. In such cases the University is neither obliged to notify the Information Commissioner of your processing nor to ensure that you adhere to the data protection principles.

Access to Personal Data by Third Parties

The University owes an obligation to its data subjects not to pass on their personal data to third parties; this may only be waived by consent, or in clearly defined circumstances. Staff may not access or disclose personal data held by the University unless such access or disclosure is for an authorised purpose in the course of their legitimate University functions. Authorised personnel should not disclose staff and student personal data available to them to other members of University staff, unless such disclosure is in accordance with authorised University business. Breaches of the University Policy on Data Protection may be the subject of disciplinary action up to, and including, dismissal from post.

Third parties, such as the police, benefit agencies and local authorities, claiming the right to access to a data subject's personal data under any of the exemptions provided in the 1998 Act, or any other exemptions provided by the Secretary of State or amending legislation, should be requested to direct their enquiry to the University Data Protection Officer.

Archiving of University Data

Notwithstanding the general requirement that data not be kept for longer than necessary for the purpose for which it was collected, the 1998 Act does allow for administrative records to be retained permanently for research purposes. The Librarian is responsible for the selection and preservation of University records, and for making them available for research and administrative purposes. Please contact the Librarian for advice on the kinds of records to be transferred.

Computing Facilities

If you are using University computing facilities, you are required to comply with the University *ITS Regulations and Guidelines* including those regarding Data Protection. Details of these Regulations and Guidelines are available from the Portal.

Examinations

With the exception of those parts of the examination process that are specifically exempted by the 1998 Act, all personal data produced and processed for the purpose of examinations and assessment may be obtained by a data subject via a data subject request. Thus, while the University is under no obligation to permit students to have access to either original scripts or copies of the scripts or to find out examination marks before those marks are actually announced, students are entitled to internal and external examiners' comments on examination scripts and assessed work with an indication of the comments' relevance to the script. Students may also be entitled to personal data drawn from minutes of Examination Boards that contain discussion about them where they are named, or referred to by identifiers from which they may be identified (such as PINs), unless the data cannot be disclosed without additionally disclosing personal data about a third party.

References

Under the 1998 Act, the University is not required to disclose references written on its behalf by members of staff. However, these references may be disclosed to a data subject by the organisations receiving them. References should therefore always be written on the assumption that the data subject may gain access to them, but you should also include a statement within the reference as to whether or not you agree to the disclosure of its contents.

Security

Data subjects may sue for compensation if they have suffered damage because personal data held by the University has been lost or destroyed or disclosed without authorisation, including unauthorised access to computer systems, or use of personal data by staff for unauthorised purposes.

Wherever possible, records concerning students and staff should be held on central systems. A minimum amount of supplementary information may be kept on Departmental sub-systems. Personal information concerning staff should be kept securely by the relevant line manager.

Individual academic staff should refrain from keeping their own records of individual students, either on paper or on personal computer, wherever possible. Such records as are kept should be deleted as soon as they cease to be relevant. Supervisors may be in possession of sensitive personal data not available to other members of the Department and should keep such information securely.

In general, you should ensure that any personal data collected, processed, or held by you in the course of your University employment

- is subject to a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
- has its security is assured no matter where or by whom data is stored or processed and throughout the whole procedure, including the transmission of data.

The following steps are suggested:

- Personal computers that hold, or can access systems containing, personal data should not be accessible to unauthorised users.
- Files containing personal data should be password-protected and encrypted where appropriate.
- You should log out of systems when you are not using them, and should log-out, or use a passworded screensaver, when leaving a computer unattended, especially during work breaks and overnight.
- Files containing personal data should be backed up routinely. Back-up storage should be physically distant from the computer.
- If your office is open to staff, students or members of the public, care should be taken to ensure that they do not have access to personal data, for example, they should not be able to view personal data on computer screens
- You should ensure that you do not retain superfluous copies of data, which may become out-of-date and subject to error, and overlooked in the normal course of data handling. Files (including e-mail) that are no longer required should be routinely deleted.
- You should challenge, or report to security, individuals without proper credentials who are found in areas where personal data is held or processed.

Reasonable precautions must be taken when transferring personal data in either hardcopy or electronic form. You should not assume that documents transferred by electronic means, such as e-mail and FTP, are secure, and thus information containing personal data, and in particular sensitive personal data, should either not be transferred by these means or should be encrypted before transmission. Personal data sent in hardcopy form should also be transferred in a manner appropriate to its sensitivity.

Off-site processing of personal data in manual or computerised form presents a potentially greater risk of loss, theft or damage to personal data. You should thus be aware of both the institutional and the personal liability that may accrue from your off-site use of personal data. If you collect, process or hold personal data off-site you should:

- take reasonable precautions to ensure that the data is not accessed, disclosed or destroyed as a result of act or omission on your part.
- ensure personal data held in manual form is stored as securely as possible, and ideally is locked away when not in use.
- have an up-to-date virus-scanning program installed on laptop computers or personal machines and scan all disks, e-mails, and other potential virus vectors for viruses.
- back up system hard drives to avoid loss of data.
- report all computer security incidents including virus infections to the institution

You should take particular care when using laptop computers offsite. It is suggested that you

- keep the laptop constantly in view when travelling, especially in busy places/terminals such as airports;
- do not check the laptop as baggage unless it is placed inside luggage that has been locked
- notify the institution immediately in the event of loss or theft

You should ensure the proper disposal of personal data when it is no longer required. The method of disposal should be appropriate to the sensitivity of the personal data to be destroyed. The minimum standard for the destruction of paper and microfilm documentation should be shredding. The minimum standard for the destruction of data stored in electronic form should be reformatting or overwriting, and electronic storage media containing sensitive personal data should be overwritten to a suitable standard or destroyed. You should note that that erasing electronic files on many computer operating systems does not equate to destroying them.

Further Information

The University's Data Protection Officer is the Librarian. He can be contacted on telephone 7306 and email David.Farley@winchester.ac.uk. He can provide copies of the University's full policy on Data Protection, and may be able to assist with further questions.

The Information Commissioner has a website with further information about both the Data Protection Act 1998 and the Freedom of Information Act 2000.
<http://www.dataprotection.gov.uk/>

The Joint Information Systems Committee of the HEFCE has produced guidance on Data Protection for the HE sector, and the University of Lancaster has developed a set of good practice pointers based on these Guidelines.

<http://www.jisclegal.ac.uk/LegalAreas/DataProtection.aspx>
<http://www.dpa.lancs.ac.uk/>

Other Relevant University Documentation

The University of Winchester Data Protection Policy
Data Protection Guidelines: Students
Subject Access Request Form and Guidance Document
ITS Regulations and Guidelines

THE DATA PROTECTION ACT 1998

DATA PROTECTION GUIDELINES: STUDENTS

Introduction

The Data Protection Act 1998 governs the ways in which data relating to individuals may be processed. In the context of the the University of Winchester, this applies to any information relating to individuals, which may be held in any office, or by any staff member, of the University.

The University expects its members not only to comply with the legislation but to safeguard personal information in accordance with best practice in the light of the principles of data protection. These Guidelines summarise the implications of data protection legislation for the University and provide a set of guidelines that deal with individual points in more detail. Members of the University who are unclear about the data protection implications of any aspect of their work should seek the advice of the University Data Protection Officer.

The University was registered under the Data Protection Act 1984. This registration will be continued in an appropriate form under the Data Protection Act 1998. The registration may be accessed via the web pages of the Office of the Information Commissioner or on application to the University Data Protection Officer. The University has a Data Protection Policy, which is available for consultation at the Portal.

Definitions

"Personal data" - "Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.

"Sensitive personal data" - The 1998 Act distinguishes between "ordinary personal data" such as name, address and telephone number and "sensitive personal data" including 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 such data is subject to much stricter conditions.

"Processing" – the obtaining, recording or holding information or data or carrying out any operation or set of operations on information or data, including; organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or; alignment, combination, blocking, erasure or destruction of the information or data;

"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 personal data are processed and the way in which the personal data are processed.

"Data subject" - A "data subject" is an identifiable or identified living individual who is the subject of personal data.

"Data subject access"- "Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
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 in relation to the purpose or purposes for which they are processed.
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 EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Your Rights

You are entitled to have access to information held about you by the University, except where releasing that information would breach another person's privacy, and subject to other exemptions contained in the 1998 Act. You also have rights including rights to

- prevent processing likely to cause damage or distress;
- prevent processing for the purposes of direct marketing;
- request that inaccurate data held on you by the University, and any other personal data in respect of which the University is the data controller and which contain an expression of opinion which appears to be based on the inaccurate data, is rectified, blocked, erased or destroyed.

It is the University's policy to seek consent whenever practicable from individual data subjects for the main ways in which the University may hold and process personal data concerning them. Although many types of personal data may, at the discretion of the University, be fairly and lawfully processed by the University under the 1998 Act without the need to obtain data subjects' consent, the obtaining of consent is the simplest way of ensuring that all parties are aware of their rights and obligations under the Act. This also allows individuals to raise any objection to the intended processing of their personal data. The University will consider any objections, but reserves the right to process personal data in the absence of consent, where such processing is permitted by reason of fulfilling one of the criteria within Schedule 2 of the Data Protection Act, for example, where the University needs to process personal data to carry out legitimate University functions, or in order to comply with a legal obligation. You will be asked to sign a consent form that will identify the personal information the University will hold on you in support of its general business functions.

Subject Access Requests

As a matter of policy, the University will normally make certain parts of the personal data held on you accessible on request. This data includes:

- Details of your application to the University and how it was considered
- Details of the information used by Examination Boards to decide on progression or graduation issues (such as marks or concessions information)
- Details of information sent to sponsoring organisations such as your LEA and postgraduate award bodies such as research councils.
- Details of the information used in disciplinary or appeals hearings – these will normally be provided to all parties involved.

However, under the 1998 Act you are also entitled to make what is know as a "subject access request" to access and obtain in permanent form a copy of any personal data held on you by the University that is not subject to exemption by the Act. If you wish to make a subject access request, your request must be:

- made in writing (this may be in electronic form)
- accompanied by a fee of £10

Before we can act on your request, we must:

- be sure of your identity
- be supplied with information from you in order to locate the information you seek

You are entitled:

- to be informed whether your personal data are being processed by the University
- to have the information constituting the personal data communicated to you

You may apply to access your data in writing in any way you choose. A Subject Access Request Form and Guidance document is available from the University Data Protection Officer for your convenience.

On receipt of your completed request and payment of the fee, the University is obliged to respond in 40 days. This period may be extended if we need further information from you. The information that we give to you will include an explanation of any codes contained in it. The data will be in its latest form.

If you have any reason to believe that the University has not dealt correctly with your request, please first take the matter up with the University Data Protection Officer. If you remain unsatisfied after discussion with the University Data Protection Officer, you should raise a complaint under the University's Complaints Policy. If you remain unsatisfied you should then contact the Information Commissioner who is officially appointed to consider such complaints. Her address is: Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Your Responsibilities

You must ensure that any personal data provided to the University is accurate and up-to-date. Please inform Registry of changes of address or other personal details.

If you are using University computing facilities, you are required to comply with the University *ITCS Regulations and Guidelines* including those regarding Data Protection. Details of these Regulations and Guidelines are available from the Portal

Specific guidance on the use of personal data in academic research is contained in the University document *The Data Protection Act 1998: Use of Personal Data in Research* available from the Portal.

Further Information

The University's Data Protection Officer is the Librarian. He can be contacted on telephone 7306 and email David.Farley@winchester.ac.uk. He can provide copies of the University's full policy on Data Protection, and may be able to assist with further questions.

The Information Commissioner has a website with further information about both the Data Protection Act 1998 and the Freedom of Information Act 2000. http://www.dataprotection.gov.uk/

The Joint Information Systems Committee of the HEFCE has produced guidance on Data Protection for the HE sector, and the University of Lancaster has developed a set of good practice pointers based on these Guidelines. http://www.jisclegal.ac.uk/LegalAreas/DataProtection.aspx http://www.dpa.lancs.ac.uk/

Other Relevant University Documentation

The University of Winchester Data Protection Policy

Subject Access Request Form and Guidance Document
ITS Regulations and Guidelines

Approved by Planning and Resources Committee on 1 February 2011

THE DATA PROTECTION ACT 1998

FREQUENTLY ASKED QUESTIONS

1. What is the Act about

The Data Protection Act 1998 places obligations on the University and its employees and students. To comply with the Act, personal data must be collected and used fairly, stored and disposed of securely and not disclosed to any unauthorised person.

2. How does the new Act affect me?

If you collect, store or process personal data, the Act requires that you undertake these functions in compliance with the terms of the Act. Personal data must be collected and used fairly, stored and disposed of securely and not disclosed to any unauthorised person. The new Act extends to manual (i.e. non-computerised) as well as computerised files. This means that paper files, card index and other record systems which contain data about identifiable living people is subject to the Act. Information could be required to be disclosed to the individual concerned. Staff, students, and alumni may have to give you permission for the collection, storage, processing and disclosure of personal data.

3. How do I get permission to process data?

From the start of the 2002/3 session, staff and students are asked to consent to the processing of certain types of personal data for certain purposes. This should cover nearly all of the data that staff will be required to deal with. See the relevant documents on the Portal for details. Other data should not be processed without the specific permission of the people concerned. If in doubt, seek the advice of the University Data Protection Officer.

4. I have been asked by a student to supply a copy of their records. What should I do?

Refer the request to the Director of HR and Registry. The student will be asked to complete and return a form setting out the information they wish to see. They will also have to pay a fee which is currently £10. The University has to provide the information to the student within 40 days of the completed request form and cheque being received.

5. What about exam marks and results?

Exam scripts themselves are exempt from disclosure but marks should be disclosed. In addition, if such a request was received, minutes from an exam board meeting relating to a particular student, together with details of examiners' comments could be subject to disclosure.

6. Can we still publish degree results on notice boards and in degree ceremony booklets etc. ?

Provided there is nothing which would enable individual students to be contacted (e.g. by the inclusion of e-mail or postal addresses or telephone numbers) then this does not breach the new Act. However, if individual students were to indicate that they did not wish their names to be included on the published list, this should be respected.

7. What about registration under the new Act?

The University has a blanket registration which covers all the functions of the University.

8. I want to create a photoboard showing photographs of all staff and students within my Department. Can I do this?

Permission to use of photographs for a range of academic functions is included in the Student and Staff Consent Forms.

9. I want to publish a list of students' email addresses/home addresses on the Faculty notice board. Can I do this?

Consent must be obtained from all the individuals concerned before any such personal data is made public. If an individual does not consent then their data must not be published. If an individual initially agrees but then changes their mind, their data must be removed.

10. I have obtained consent to display certain items of personal data on the notice board/in a handbook. Can I also publish the information on my website?

Only if you have also obtained consent to this from the individuals concerned. You cannot assume that consent for a particular use of data extends to any other use. If you have consent to use data for a particular purpose and wish to use this data for a further or different purpose, additional consent must be obtained from all the individuals concerned. This is particularly important in relation to the worldwide web because of the universal accessibility of information published on it.

11. I am already holding information on a database of contacts which I have compiled over a number of years. Can I continue to hold this information?

Yes, but you should think about what data you are holding and why. The information should be relevant, kept up to date and held for no longer than necessary. If you have old or unreliable information you should either update or delete it. One way to do this would be to write to the individuals concerned notifying them of the information you hold and asking them to check that it is correct. You can also then notify them of the purposes for which the data is held and seek their consent.

12. I have sent literature about forthcoming events, reunions etc. to past students. A couple of people have objected, saying that they do not wish to receive any further communications. What should I do?

You must ensure that these persons are not sent any further communications. If mail is generated by computer you must have a system in place ensuring that people who have objected to receiving communications are removed from your mailing list.

13. Some of our files contain comments of a personal or derogatory nature. Could these be disclosable to the individual concerned?

Yes – potentially all information could be disclosed. The general rule is that if you would be embarrassed by a person seeing comments made about them then you should not make those comments.

14. What about confidential information such as references. Could they have to be disclosed?

Potentially yes. There are complicated rules about references but basically although the subject of the reference cannot require a copy from the person giving the reference, they could possibly obtain it from the person the reference was provided to.

15. I have been contacted by a third party requesting information about a student/member of staff. What should I do?

The general rule is not to disclose information about a student or member of staff to a third party outside of the University without the consent of the person having been obtained. In most cases, consent from the student/member of staff should be obtained before information is disclosed, although this may not be

possible, e.g. in the case of a medical emergency. If you are in any doubt as to whether information should be disclosed please contact the University's Data Protection Officer.

16. I have a form/questionnaire which students/staff/third parties complete and return. Do I need to modify this because of the new Act?

Yes. Please refer to the advice on the Data Protection Act web page on the University's website or seek advice form the Data Protection Officer who will be able to help with the drafting. Basically such forms should tell the recipients what their data will be used for, where it will be held and to whom it may be disclosed.

17. What about records. How long should I retain them?

Data should be held for no longer than is necessary. The University has guidelines for the retention of records. Advice should be sought form the Data Protection Officer. In general, it is good practice not to amass more personal information about individuals than necessary, to discard irrelevant or out of date information and to destroy unnecessary duplicates or photocopies.

18. This all seems quite complicated. Is there a basic rule I should remember?

Be careful about the information you hold and in particular who you pass it to. Think about what you are using data for and whether this is what the individual would expect you to use it for. Think whether it is covered by the general consent provided by staff and students (above).

19. Who should I contact if I need further help?

The University's Data Protection Officer, currently the Librarian.

THE DATA PROTECTION ACT 1998

STUDENT AND ALUMNI RECORDS: CONSENT FORM

Approved by Planning and Resources Committee on 1 February 2011

The University of Winchester holds personal data on students, past and present, in electronic form on its Student Records, Library, IT, Finance, Accommodation and Alumni systems and in paper form in certain structured manual files. To assist the University to comply with its legal obligations under the Data Protection Act 1998, the aim of this document is to explain what data is held and the purpose or purposes for which it will be processed and disclosed. Full details of the University's notification to the Office of the Information Commissioner (OIC) can be obtained from the University Data Protection Officer or from the OIC directly.

Although many types of personal data related to your studies at The University of Winchester may, at the discretion of the University, be fairly and lawfully processed by the University under the 1998 Act without the need to obtain your consent, the obtaining of consent is the simplest way of ensuring that all parties are aware of their rights and obligations under the Act.

Please would you sign at the end of the form to indicate your consent to the University processing your personal data for the specified purposes. If you object to any of the processing indicated then you should attach a document to this form indicating this, and your objection will be considered. All students will be advised on where to access guidance on the University's data protection policy, which outlines an individual's rights and obligations under the 1998 Act. If you have any queries about the University's data protection policy, please contact the University Data Protection Officer

The University processes personal data for purposes in connection with:

Applications
Enrolment
Academic Progression
Assessment
Discipline
Accommodation
Student welfare and related support services
Immigration procedures
Careers services
Employment, including references
Work and other placements
IT systems
Library
Financial records
Alumni

The types of data that are processed for those purposes include:

- Previous academic attainment
- Previous employment, skills, experience and training
- Mental or physical health, including dates of absence from University due to illness and the reason for absence
- Matters relating to health
- Criminal convictions
- Data for monitoring equal opportunities, e.g. race, ethnic origin, gender, disability and age
- Qualifications
- Matters of Discipline
- Matters relating to residential including smoking/noise
- Assessment grades and marks
- Fees status
- Residential status
- Nationality
- Financial data
- Contact addresses
- Matters relating to student welfare and related support services
- Immigration information
- CCTV images
- Photographs and video images

The personal data may be provided by individuals themselves (e.g. by way of application and enrolment forms) and also by third parties such as schools, local authorities, examination boards and sponsors.

In order to ensure the proper functioning of the University as an institution in the higher education sector, the University may from time to time, consider it appropriate to disclose relevant personal information about students, past and present, within the University to members of staff, committees and organisations (e.g. the Students Union), and also to various external bodies including other educational institutions, employers and potential employers, professional bodies, funding bodies, local authorities and other government and regulatory bodies. The University may or may not seek further consent to specific disclosures depending upon the intended disclosure.

The University will usually seek to maintain contact with its alumni. All personal data supplied by alumni of the University will be held by the Alumni Office on a secure and confidential basis.

The University may process alumni personal data for purposes in connection with:

- Sending University newsletters and reports.
- Information on products and services of potential interest to alumni in University mailings
- Requests for fund-raising, via mail and telephone.
- Requesting non-financial support from alumni, e.g. career advice.
- Processing enquiries relating to alumni who have lost contact with others.
- Inviting alumni to reunions and other events.

The types of data that are processed for those purposes include:

- Addresses
- Years of study
- Qualifications obtained

Alumni are entitled to request that where their personal data are collected and processed for alumni contact purposes, the data are not also processed for direct marketing purposes. They may also obtain the rectification, blocking, erasure, and destruction of personal data held by the University. Any objection to the use of personal data by the University for the purposes of alumni contact or direct marketing should be provided to the University Data Protection Officer in writing.

Some types of personal data are treated as particularly sensitive by the Data Protection Act 1998. In the absence of specific legislative conditions, explicit consent is required in order that such data may be fairly and lawfully processed. By signing this form you are indicating your explicit consent to the processing of sensitive personal data as set out below.

Ethnic origin - The University may process information provided by a student about their ethnic origin for the purposes of equal opportunity monitoring, but only in an anonymised form, and may disclose such statistics to external bodies. The University will not otherwise disclose any information about a student's ethnic origin except with the student's explicit consent to the proposed disclosure or in other circumstances permitted or required by law.

Criminal records - The University needs to process this data in order to protect the staff and the other students of the University, to operate a proper disciplinary procedure, to assist with the provision of references and to comply with any legal obligations. The University may receive information about a student's criminal record or allegations of a criminal offence from the student or from external sources such as the police and the Criminal Records Bureau. The University may be permitted by law to disclose such information to other external bodies with out the student's explicit consent (e.g. where the proposed disclosure is necessary to protect the vital interest of another person).

Medical records and data - The University needs to process this data in order to acquire necessary sickness or disability data that may be required to make determinations about a student's academic performance (e.g. the provision of anonymous information to examination boards about special circumstances affecting exam performance), to facilitate obligations pursuant to disabilities legislation and to assist with any dietary and accommodation requirements. Any medical data provided to the University by or about a student will be held in accordance with the principles of medical confidentiality. Such personal data shall be disclosed to such University members as the University considers necessary, but shall not be disclosed outside the University except with the student's explicit consent to the proposed disclosure or in other circumstances permitted or required by law (e.g. to protect the vital interests of the student). The University may inform the student's "emergency contact" of necessary medical information in such circumstances.

DECLARATION - I give my written consent that the University may process and disclose relevant personal data as set out above, including the processing of sensitive personal data for the purposes specified. My consent is conditional upon The University of Winchester complying with its obligations and duties under the Data Protection Act 1998

I attach a document with any objections to the processing of my personal data [ ] *Please tick if applicable.*

Signed …….. Date ……..

Name …… (Block Capitals Please)

Approved by Planning and Resources Committee on 1 February 2011

THE DATA PROTECTION ACT 1998

STAFF RECORDS: CONSENT FORM

The University of Winchester holds personal data on staff in electronic form on its Personnel, Library, IT and Finance systems and in paper form in certain structured manual files. To assist the University to comply with its legal obligations under the Data Protection Act 1998, the aim of this document is to explain what data is held and the purpose or purposes for which it will be processed and disclosed. Full details of the University's notification to the Office of the Information Commissioner (OIC) can be obtained from The University Data Protection Officer or from the OIC directly.

Although many types of personal data related to your employment may, at the discretion of the University, be fairly and lawfully processed by the University under the 1998 Act without the need to obtain your consent, the obtaining of consent is the simplest way of ensuring that all parties are aware of their rights and obligations under the Act.

Please would you sign at the end of the form to indicate your consent to the University processing your personal data for the specified purposes. If you object to any of the processing indicated then you should attach a document to this form indicating this, and your objection will be considered. All staff will be advised on where to access the University's data protection policy, which contains further guidelines and outlines an individual's obligations. If you have any queries about the University's data protection policy, please contact the University Data Protection Officer.

The University processes personal data for purposes in connection with:

- Payments due under the contract of employment
- Monitoring of leave and absence
- Training and development purposes
- Management planning
- Negotiations with the trade union or staff representatives
- Redundancy
- Curriculum planning and organisation, and timetable organisation
- Provision of information and statistics under statutory authority to Government bodies
- Equal Opportunities Monitoring
- Compliance with the Disability Discrimination Act
- Carrying out checks through the Criminal Records Bureau or other appropriate mechanisms
- IT accounts
- Security
- Other requirements to assist with the good management of the institution

The types of data that are processed for those purposes include:

- Previous employment, skills, experience and training
- Mental or physical health, including dates of absence from work due to illness and the reason for absence
- Matters relating to pregnancy, maternity, paternity, parental and any other paid or unpaid leave
- Criminal convictions
- Data for monitoring equal opportunities, e.g. race, ethnic origin, gender, disability and age
- Qualifications
- Matters of Discipline
- Pensionable pay or contributions
- Length of service
- Membership of recognised trade unions
- Current employment, grade, remuneration and emoluments
- Internal Responsibilities / Membership of University Committees
- External Responsibilities
- Specialist Academic Interests
- Research Undertaken
- Publications
- Conferences attended
- CCTV images
- Photographs and video images

The University may from time to time, where the processing of personal data is necessary for the performance of your duties, or the proper functioning of the University, consider it appropriate to disclose relevant personal data to external bodies including other educational institutions, other employers and potential employers, professional bodies, funding bodies, local authorities and other government and regulatory bodies. The University may or may not seek further consent to specific disclosures depending upon the intended disclosure.

In order to assist with the proper functioning of the University, the University may provide or publish employees' University telephone number, University address, e-mail address and appropriate information about their University duties, whether in hard copy and electronic directories, upon enquiry, or on such websites as are approved by the University from time to time. Any objection to the provision of such details by the University in such circumstances should be given to the University Data Protection Officer, in writing, for consideration.

Some types of personal data are treated as particularly sensitive by the Data Protection Act 1998. In the absence of specific legislative conditions, explicit consent is required in order that such data may be fairly and lawfully processed. By signing this form you are indicating your explicit consent to the processing of sensitive personal data as set out below.

Medical records and data - The University needs to process this data in order to keep proper sickness records, to assist in providing healthcare and staff welfare, to facilitate obligations pursuant to disabilities legislation and to assist with any dietary and accommodation requirements. Any medical data provided to the University by or about a member of staff will be held in accordance with the principles of medical confidentiality. Such personal data shall be disclosed to such University members as the University considers necessary, but shall not be disclosed outside the University except with the member of staff's explicit consent to the proposed disclosure or in other circumstances permitted or required by law (e.g. to protect the vital interests of the member of staff). The University may inform the member of staff's "emergency contact" of necessary medical information in such circumstances.

In order to administer the occupational sick pay and leave scheme all staff are required to provide information about their absences and the reasons for them. In some cases this will be by way of self-certification. Refusal to provide this information and to give consent for the University to process it will result in the cessation of sick pay until such time as the information is provided and the consent given.

Ethnic origin - The University needs to process this data in order to assist with any dietary requirements and to identify possible sources of financial assistance. The University may also process information

provided by a member of staff about their ethnic origin for the purposes of equal opportunity monitoring, but only in an anonymised form, and may disclose such statistics to external bodies. The University will not otherwise disclose any information about a member of staff's ethnic origin except with the member of staff's explicit consent to the proposed disclosure or in other circumstances permitted or required by law.

Criminal records - The University needs to process this data in order to protect the other staff and the students of the University, to operate a proper disciplinary procedure, to assist with the provision of references and to comply with any legal obligations. The University may receive information about a member of staff's criminal record or allegations of a criminal offence from the member of staff or from external sources such as the police and the Criminal Records Bureau. The University may also be obliged by law to disclose information about a member of staff's criminal offences or allegations of criminal offences to other external bodies, such as the police, in certain circumstances. The University may also be permitted by law to disclose such information to other external bodies without the member of staff's explicit consent (e.g. where the proposed disclosure is necessary to protect the vital interest of another person)

Declaration

I give my written consent that the University may process and disclose relevant personal data as set out above, including the processing of sensitive personal data for the purposes specified. My consent is conditional upon The University of Winchester complying with its obligations and duties under the Data Protection Act 1998

I attach a document with any objections to the processing of my personal data [ ] *Please tick if applicable*

Signed …….. Date ……..

Name …… (Block Capitals Please)

Approved by Planning and Resources Committee on 27.06.02

The Data Protection Act 1998

Disclosure of Student Data to Third Parties

The University of Winchester collects a wide range of personal data relating to students for the University's own purposes, and to meet external obligations. Both these types of collection by the University may result in the eventual disclosure of personal data to third parties by staff. Such disclosure is permitted where students have given their consent to the transfer, or in those circumstances where the 1998 Act expressly permits transfers without such consent. Consent cannot be inferred from silence, thus if the University requests that consent be given by students in order that the University can provide personal data to a third party, and no communication from a student is forthcoming, staff must infer that consent is withheld.

> "Personal data" - "Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.
>
> "Sensitive personal data" - The 1998 Act makes a distinction between what might be termed "ordinary personal data" e.g. name, address and telephone number and "sensitive personal data" including 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 and disclosure of such data is subject to much stricter conditions.

Student personal data includes, but is not limited to:

- their Winchester address and other contact details, including e-mail address.
- their academic record, including exam results, submission of written work, and attendance at classes

Students may also not wish the fact of their attendance at the University to be disclosed, particularly where they are estranged from family members, or have concerns about stalkers. Staff should refuse to confirm whether a student is registered with them or not without the student's consent except in the cases detailed below covering release of data to third parties.

Staff should be aware that as a data controller, the University therefore owes an obligation to students not to pass on their personal data to unauthorised third parties, which may only be waived by consent, or in clearly defined circumstances. Unauthorised third parties will include:

- A person or organisation to whom the data subject has not consented that the data be disclosed, unless the 1998 Act expressly permits such transfers without such consent;
- A person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given, unless the 1998 Act expressly permits such transfers without such consent.

"Unauthorised third parties" will include family members, friends, local authorities, government bodies, and the police, unless disclosure is exempted by the 1998 Act, or by other legislation. There is no general legal requirement to disclose information to the police.

Data may be disclosed to third parties without consent in situations where it is required for the:

- purpose of protecting the vital interests of the data subject (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject);
- purpose of preventing serious harm to a third party that would occur if the data were not disclosed;
- purpose of safeguarding national security;
- prevention or detection of crime;
- apprehension or prosecution of offenders;
- assessment or collection of any tax or duty or of any imposition of a similar nature;
- discharge of regulatory functions, including securing the health, safety and welfare of persons at work.

With regard to the final 4 categories, it should be noted that disclosure is allowed in those cases only to the extent to which failure to disclose would be likely to prejudice the attainment of those aims.

Third parties claiming the right to access to a data subject's personal data under any of the exemptions described above, or any other exemptions provided by the Secretary of State or amending legislation, should normally be requested to direct their enquiry to the University Data Protection Officer.

With regard to situations where employment agencies or prospective employers contact staff to verify details about a student, such as attendance records, examination results, and degree classifications, in most circumstances, students would not object to the disclosure of such information, and indeed this would appear to benefit students. However, care should be taken to ascertain that the third party has a genuine requirement for the information, and thus, for example, telephone disclosure would appear to be unsatisfactory, as verification of identity in such circumstances is difficult. Ideally, the request for the disclosure of the details to the third party should either come from the student directly, or the request from the third party should be accompanied by a statement from the student consenting to the disclosure.

For advice on writing references for students, staff should refer to *Reference Writing Guidelines for Staff and Students* on the Portal.

Guidelines

Unless members of staff are aware that a student has consented to their personal data being released to a third party (including family members), or in all the circumstances, it is reasonable to believe that the data is immediately required to protect the vital interests of the student, or prevent serious harm to a third party, they should **not** disclose a student's personal data. Third party requests other than those from parents, relatives and guardians of students should normally be routed via the University Data Protection Officer.

The legal restrictions upon the University's ability to disclose personal data to third parties should be explained as clearly as possible to parents, relatives and guardians of students when requests for personal data are made. The University is not '*in loco parentis*' and owes no legal obligation for its staff to disclose information about a student to family members. Disclosure of a student's personal data in breach of the 1998 Act could potentially expose the University to legal action.

Where a student has signed a consent form permitting the disclosure of their personal data to a third party, it should be remembered that consent, once given, may be withdrawn at a later date. Where a student purports to withdraw a written consent, it is best if that withdrawal is also in writing.

When members of staff receive enquiries as to whether a named person is a student in the University, the enquirer should be asked why the information is required. If the reason is not one that would justify disclosure, the member of staff should decline to comment one way or the other.

If a request for information about a student is refused, but the subject matter of the enquiry is evidently of importance to the student, the student should be informed as soon as possible of the enquiry. This will allow the student to contact the enquirer should they so wish.

Where a University employee requests personal data about a student, such information should be released only if, and only to the extent that, they require the information in order to perform their official duties.

Enquiries from Embassies and High Commissions should be treated with extreme caution. Students may choose to have little or no contact with representatives of their home states, the extent of the relationship is a matter for the student, not the staff member, to determine. Representatives of foreign governments are entitled to information only when they are sponsoring students. They may not be given wholesale lists of students who are their nationals. Sponsors are entitled to periodic reports on the student's academic progress. They may not have access to other personal data such as the student's address.

As a matter of good practice, student personal data should not be disclosed over the telephone, as verification of the third party is extremely difficult in such circumstances. As an alternative to divulging personal data, the University may be willing to accept a sealed envelope which it will attempt to forward to the student's last-recorded address, or to forward an incoming email message to a student.

Approved by Planning and Resources Committee on 1 February 2011

THE DATA PROTECTION ACT 1998

USE OF PERSONAL DATA IN RESEARCH

1. Introduction

The University of Winchester seeks to ensure that all research carried out under its auspices, whether by staff, post-graduate or undergraduate students, conforms with both the letter and the spirit of all legislation relating to such research, and particularly according to the principles and guidance for good practice of the Data Protection Act (1998). The guidelines below present a digest of the Data Protection Act as it currently applies to the use of personal data in research, and some advice and checklists for researchers. All persons undertaking research as part of their employment and/or study courses at The University of Winchester are expected to familiarise themselves with the provisions of the Act in relation to their own research purposes and methods, and to seek advice from the University Data Protection Officer in cases where they are unclear as to their responsibilities in relation to the Act. In addition, researchers are strongly advised to consult the *Code of Practice for Research* produced by the relevant professional or subject association in relation to the specific area in which research is being undertaken.

The Data Protection Act 1998 came into force on 1 March 2000. It sets out conditions for the legal processing of personal information and applies to paper records as well as those held on computers.

Many research projects carried out in the HE sector, both those carried out by staff as part of their academic, administrative, or service work, and those carried out by students in the course of their studies, will involve the processing of information relating to identifiable living individuals. Researchers should be aware that such processing constitutes 'personal data processing' and is subject to the provisions of the Data Protection Act 1998, including the eight data protection Principles.

The 1998 Act explicitly provides for the processing of personal data for research purposes in the Part IV Exemptions, even where the personal data to be processed were not collected for that purpose. However, researchers have to observe certain conditions before their processing will be considered fair and lawful.

This document outlines the conditions for the lawful use of personal data by researchers, and includes a data protection checklist for proposed research projects.

2. Definitions

"Personal data" - "Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.

"Sensitive personal data" - The 1998 Act distinguishes between "ordinary personal data" such as name, address and telephone number and "sensitive personal data" including 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 such data is subject to much stricter conditions.

"Processing" – the obtaining, recording or holding information or data or carrying out any operation or set of operations on information or data, including; organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or; alignment, combination, blocking, erasure or destruction of the information or data;

"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 personal data are processed and the way in which the personal data are processed.

"Data subject" - A "data subject" is an identifiable or identified living individual who is the subject of personal data.

"Data subject access"- "Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

3. The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met
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 in relation to the purpose or purposes for which they are processed.
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 EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. The Conditions

The conditions for the use of personal data in the course of research are contained in s.33 of the Data Protection Act 1998, and s.9 of the Data Protection (Processing of Sensitive Personal Data) Order 2000 (see annex below).

4.1 Definition of Research

The 1998 Act does little to define the term "research purposes", except to state that it includes "statistical or historical purposes." However, it would seem reasonable to assume that research projects at HE institutions carried out by staff as part of their academic employment, or carried out by students in the course of their studies, would normally fall within the understood definition of 'research purposes'.

4.2 Notification of Processing

Where employees at The University of Winchester process personal data for which the University is Data Controller, as a legitimate part of their employment (e.g. research, teaching, consultancy and administration), they may usually rely upon the notification to the Information Commissioner provided by the University. It is, however, important that researchers inform the University Data Protection Officer of their intention to process personal data for research purposes, and ensure that their processing remains in

compliance with the 1998 Act. Breaches of the Act in such circumstances may lead to disciplinary action by the University.

Where employees process personal data for which the University is not Data Controller, e.g. processing for the purposes of research unrelated to their University employment, this processing may require notification to the Information Commissioner by the employee or employees concerned. In such cases the University is neither obliged to notify the Information Commissioner of the processing nor to ensure that the data protection principles are adhered to.

In cases where students are processing personal data within HE and FE institutions, for which the University is Data Controller, then the students conducting the research, or engaged in the course of study, can usually rely upon the notification to the Information Commissioner provided by the University. It is, however, important that students inform their supervisors of their intention to process personal data for research purposes, and ensure that their processing remains in compliance with the 1998 Act. Supervisors should ensure that students are aware of the requirements of the Act, in particular those provisions relating to research. Breaches of the Act in such circumstances by students may lead to disciplinary action by the University.

Where students process personal data for which the University is not Data Controller, e.g. processing for the purposes of research unrelated to their studies, this processing may require notification to the Information Commissioner by the student or students concerned. In such cases the University is neither obliged to notify the Information Commissioner of the processing nor to ensure that the data protection principles are adhered to.

4.3 Research Purposes

Where personal data is to be processed under the s.33 exemption for research purposes, that processing is permitted, provided that it is carried out exclusively for those research purposes. Additionally, the data to be processed may not be:

- processed to support measures or decisions relating to particular data subjects
- processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

If the research purposes exemption applies:

- the further processing of personal data will not be considered incompatible with the purposes for which they were obtained (exemption from Principle 2);
- personal data may be kept indefinitely (exemption from Principle 5);
- subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form that identifies data subjects (exemption from Principle 7 and Section 7 of the Act).

Even where a researcher can demonstrate that his/her project meets the requirements of the research purposes exemption, they are still required to comply with the rest of the Act, including Principles 1 & 2. The data controller should, therefore, ensure that, at the time the data are collected, the data subject is made fully aware of what the data controller intends to do with the data. If the data controller subsequently decides to process the data in order to carry out further research of a kind that would not have been envisaged by the data subject at the time the data were collected, the data controller will need to comply with the fair processing requirements of the Act in respect of this further processing

The exemption will not be lost just because the data are disclosed –

- to any person, for research purposes only;
- to the data subject or someone acting on his behalf;
- at the request, or with the consent, of the data subject or someone acting on his behalf;
- where the person making the disclosure has reasonable grounds for believing the disclosure falls within (a), (b) or (c) above.

As a matter of good practice, when processing for research, historical or statistical purposes, data controllers should always consider whether it is necessary to process personal data in order to achieve their purpose. Wherever possible, data controllers should only process data that has been stripped of all identifying features. If the data is completely anonymised and no 'key' to the identity of the data subjects is held, or is likely to come into the possession of the data controller, then the Act will not apply as such data no longer constitutes 'personal data'.

4.4 Fair Processing of Data

Despite the exemption from Principle 2, research data subjects should still be informed of any new purposes of data processing and the identity of the data controller and any disclosures that may be made. If this involves disproportionate effort then data controllers may avoid this obligation, noting in their records the reasons for believing that disproportionate effort would be required.

Research data is exempt from Principle 2. Thus, personal data obtained for other purposes may be processed for research even if that purpose was not made explicit to data subjects. However, notwithstanding this exemption, the data subject should still be informed of any new purposes of data processing and the identity of the data controller and any disclosures that may be made (Principle 1). Such notification may be avoided if:

- The data has been obtained directly from the data subject but the purpose of processing the data for research was not known at the time and it is subsequently deemed 'not practicable' to provide the relevant information.
- The data has been obtained from a third party; and provision of such information would involve disproportionate effort; the data subject has made no prior demand for information; and the data controller records the reasons for believing that 'disproportionate effort' applies. Such reasons might include factors such as cost, time and ease of provision of information. These should be weighed against disadvantages to the individual.

4.5 Sensitive Personal Data

The processing of sensitive personal data for research purposes may only be carried out if one of the conditions in Schedule 3 of the 1998 Act is satisfied. For research purposes, the relevant conditions are likely to be:

- where the explicit consent of the data subject has been obtained.
- where medical research is being carried out by a health professional or someone who owes a similar duty of confidentiality.
- where the research is an analysis of racial/ethnic origins, carried out for the purpose of equal opportunities monitoring.
- where it has been additionally provided for by the Secretary of State. *The Data Protection (Processing of Sensitive Personal Data) Order 2000* allows for sensitive data processing which: "is in the substantial public interest and is necessary for research purposes and does not support measures with respect to the particular data subject except with their specific consent nor cause or be likely to cause substantial damage and distress." Researchers seeking to use this exemption should include a statement in the project proposal document (or equivalent) indicating the potential benefits to the public of their research.

4.6 Security of Data

The requirements for appropriate security of data (Principle 7) must be respected including appropriate levels of security for sensitive data and security of data processed by researchers outside the University.

4.7 International Research

Researchers may engage in international research collaborations requiring the transfer of personal data outside the EEA. Data may not be transferred to countries outside the EEA (Principle 8) unless that country has adequate data protection regulations, or the explicit consent of data subject has been obtained,

or there is an appropriate contract with the recipient of the data, specifying appropriate data protection requirements that must be upheld. Thus, institutions must be exceptionally careful when contemplating the transfer of research data overseas: in most cases, the only safe option will be to ensure that data subjects give explicit consent for overseas transfer during data collection.

5. Research Project Checklist.

1. Does the project require the processing of data that relates to a living individual who can be identified from those data, or from that data and other information in your possession or which are likely to come into your possession?

   YES – You will need to consider if your project falls within the 'research purposes' exemption of the Data Protection Act 1998. Continue with the checklist.

   NO – The Data Protection Act 1998 does not apply to your project and you need not continue with this checklist.

   MAYBE – If in any doubt, discuss the matter with the University Data Protection Officer (staff), or your supervisor (students).

2. Is it likely that the results of the research be used to make decisions about any of the research subjects, or is there a risk that the data subjects might suffer distress or damage as a result of the processing?

   YES – You cannot claim the benefit of the 'research purposes' exemption of the DPA1998. You should consult with the University Data Protection Officer (staff), or your supervisor (students) to see if an acceptable way forward can be found.

   NO – You can claim the benefit of the 'research purposes' exemption of the DPA1998. However, you should notify the University Data Protection Officer (staff), or your supervisor (students) of your intention to process personal data during the project. You will need to consider whether you need to make a separate notification to the Information Commissioner from that made by the University before processing.

   MAYBE – If in any doubt, discuss the matter with the University Data Protection Officer, or your supervisor.

3. Does your project require the processing of personal data consisting of information as to the racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, or criminal record (actual or alleged) of the data subject?

   YES – You will be processing 'sensitive personal data' and will need to determine whether you can meet one of the necessary conditions in section 4.5 above. If you cannot, you cannot process the data fairly and lawfully.

   NO – You will not be processing 'sensitive personal data'. If the processing is necessary for the purposes of legitimate interests pursued by the data controller, and the processing is not unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject you will have met the one of the required necessary conditions for processing 'ordinary sensitive data'. You may still wish to request the consent of the data subject to process their personal data, but this is not mandatory.

   MAYBE – If in any doubt, discuss the matter with the University Data Protection Officer, or your supervisor.

4. Was the personal data that you are going to process previously collected for another purpose?

   YES – You will need to ensure that the data subjects, if they were not informed that their data would be used for your research when it was initially collected, are now informed about the purpose of your processing, the identity of the data controller, and any disclosures that may be made, unless this would involve disproportionate effort. If you believe that informing the data subjects would involve disproportionate effort, you must note in your records the reasons for that belief.

NO – You should inform the data subjects of the purpose of the data processing, the identity of the data controller, and any disclosures that may be made.

5. Does the project require the transfer of any of the personal data outside the EEA, for instance, to other project partners?

   YES – If the country or countries to which the personal data is to be transferred has/have adequate data protection regulations (the EU Commission has a list of those countries deemed to have adequate protections), or you have the explicit consent of the data subjects to such a transfer, or you have negotiated an appropriate data protection clause in your contract with the proposed recipient of the data, specifying appropriate data protection requirements that must be upheld, you may make the transfers. If you have not met one of the above conditions you cannot lawfully transfer the data outside the EEA.

   NO – Your project is not affected by Principle 8.

If you can satisfactorily meet the requirements above, you can claim the benefit of the first part of the research exemption - the personal data can be used for the research project even if the use for research would otherwise be incompatible with the purposes for which they were obtained AND the personal data may be kept indefinitely.

6. Will the results of the research or any resulting statistics be made available in a form that identifies individual data subjects?

   YES – Data subjects will be entitled to make subject access requests to gain access to any personal data you have processed regarding them.

   NO – You can claim the benefit of the second part of the research exemption, which is that data subject access may be withheld to the personal data used in the research.

In most cases, researchers will be able to disguise the identity of research subjects in any published results. However, some reports will describe in detail an individual subject's circumstances, which may allow them to be identified by those reading the report. Researchers must be careful, therefore, to include the minimum possible personal information in reports that look at individual cases. If it proves impossible to discuss a case without identifying the individual, then that individual should normally be given the opportunity to consent to the use of their personal data before publication can go ahead.

Checklist - Final Points

Researchers wishing to use personal data should remember that the research purposes exemptions are quite narrow, and that most of the Data Protection Principles will still apply (notably the requirement to keep data secure). There should be an assessment of the legality of processing on each occasion data are provided for research purposes. Periodic assessment and audits of the nature of data protection procedures and practices in research areas should be carried out.

Researchers are advised always to provide clear guidance to data subjects whose personal data will be used in research as to why the data is being collected, and the purposes for which it will be used. Use of jargon, abbreviations and acronyms should be avoided wherever possible in any explanatory documentation.

Researchers should ensure that a suitable mechanism is in place to ensure that data subjects whose personal data is to be, or has been, processed can meaningfully exercise their right to object to the processing of that data on the grounds that it would cause them, or has caused them, significant damage or distress.

ANNEX

Data Protection Act 1998 – s.33 - Research, history and statistics.

s.33 - (1) In this section-

"research purposes" includes statistical or historical purposes;

"the relevant conditions", in relation to any processing of personal data, means the conditions-

a) that the data are not processed to support measures or decisions with respect to particular individuals, and

b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

(2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely.

(4) Personal data which are processed only for research purposes are exempt from section 7 if -

a) they are processed in compliance with the relevant conditions, and

b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed -

(a) to any person, for research purposes only,

(b) to the data subject or a person acting on his behalf,

(c) at the request, or with the consent, of the data subject or a person acting on his behalf, or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

The Data Protection (Processing of Sensitive Personal Data) Order 2000 S.I 2000/417

CIRCUMSTANCES IN WHICH SENSITIVE PERSONAL DATA MAY BE PROCESSED

[…]

9. The processing –

(a) is in the substantial public interest;

(b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act);

(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and

(d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

THE DATA PROTECTION ACT 1998

Approved by Planning and Resources Committee on 1 February 2011

DATA SUBJECT ACCESS REQUEST FORM

The following information is needed to help us provide a quick and accurate response to your request. Please complete the form and return it together with the fee of £10 to the University Data Protection Officer, The University of Winchester, Sparkford Road, Winchester, SO22 4NR.

Section 1: Details of the person requesting the information

Full Name:

Address:

Tel. No. Fax No.

E-Mail Address:

Section 2: Are you the data subject? Please circle appropriate category.

YES If you are the data subject, please supply the following:
- evidence of your identity (i.e. a certified copy of driving licence, passport, national identity card or photo-pass)
- evidence of your current address (i.e. recent utility bill)
- a stamped addressed envelope for returning your documentation.

Please continue to section 5

NO Are you acting on behalf of the data subject with their written authority? If so please enclose the original document authorising your action.
Please complete Sections 3 & 4

Section 3: Details of the data subject, if different from Section 1

Full Name:

Address:

Tel. No. Fax No.

E-Mail Address:

Section 4: Please indicate your relationship to the data subject, and explain why you need to make their request on their behalf.

Section 5: Please describe the data you require, and indicate any other information that you think may help in identifying that data.

DECLARATION: To be completed by all applicants. Please note that the provision of false or misleading information may result in prosecution.

I.....hereby certify that all the information given by me on this form and any supporting documentation are correct to the best of my knowledge. I understand that it is necessary for The University of Winchester to confirm my/the data subject's identity, and that it may be necessary to provide more detailed information in order that the University can locate the correct personal data.

I enclose the fee of £10 (cheques should be made payable to The University of Winchester)

Signature……..Date ……..

Please note that the 40 day period for subject access will not start to run until The University of Winchester has received sufficient identification and the required fee.

The following documents must be supplied with this subject access request form:

- **Evidence of your identity**
- **Evidence of the data subject's identity if you are making the request on their behalf**
- **Authorisation from the data subject to act on their behalf (if applicable)**
- **The fee of £10**
- **A stamped addressed envelope for the return of the proof of identity and authority documents**

Guidance on Requests for Access to Personal Data

What is Data Protection?

The Data Protection Act 1998 sets out rules for the processing of personal information, and it applies to some paper records as well as to those held on computer. The Act gives individuals certain rights, and imposes obligations on those who process personal information to be open about what data are collected and how they are to be used, and to abide by 8 Data Protection Principles a follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met
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 in relation to the purpose or purposes for which they are processed.
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 EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Definitions

"Data subject" - A "data subject" is an identifiable or identified living individual who is the subject of personal data.

"Data subject access"- "Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

"Personal data" - "Personal data" are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. This includes computerised data and some manual data (e.g. paper files)

"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 personal data are processed and the way in which the personal data are processed. The University of Winchester, is a data controller under the Data Protection Act 1998. Its designated representative for the purposes of the Act is the University Data protection Officer.

Yours Rights under the Act

The Act gives rights to individuals in respect of personal data held about them by data controllers. These include the rights:

- To make subject access requests about the nature of the information and to discover to whom it has been disclosed

- To prevent processing likely to cause damage or distress
- To prevent processing for the purposes of direct marketing
- To be informed about the mechanics of any automated decision-taking process that will significantly affect them
- Not to have significant decisions that affect them made solely by an automated decision-taking process
- To take action for compensation if they suffer damage by any contravention of the Act by the data controller
- To take action to rectify, block, erase or destroy inaccurate data, and
- To request the Commissioner to make an assessment as to whether any provision of the Act has been contravened.

Subject Access Requests

If you wish to make a subject access request, your request must be:

- Made in writing
- Accompanied by a fee of £10

Before the University can act on your request we must:

- Be sure of your identity
- Be supplied with information from you in order to locate the information you seek

You are entitled to:

- Be informed whether your personal data are being processed by the University
- Have the information constituting the personal data communicated to you

Failure to provide adequate proof of identity, or to provide the necessary fee, will mean that the University cannot process your request.

On receipt of a completed University Subject Access Request Form (including adequate evidence of your identity) and payment of the required fee, the University is obliged to respond within 40 days. The information that the University will supply will include an explanation of any codes contained within it. The data supplied will, in principle, be all that held at the time that the request is made, although the law permits routine amendments and deletions of data to continue between the time of the request and the time of the reply, and to this extent the data supplied may differ from that held at the time the request was made, although no special amendments or deletions will be made.

In accordance with the 1998 Act, the University reserves the right to reject repeated requests where a reasonable period has not elapsed between requests.

If you have reason to believe that the University has not dealt correctly with your access request, the matter should be taken up in the first instance with the University Data Protection Officer. If you remain unsatisfied after discussion with the University Data Protection Officer, you should raise a complaint under the University's Complaints Policy. If you remain unsatisfied you should then contact the Information Commissioner who is officially appointed to consider such complaints. The address is: Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Contact information

All requests for access to personal information should be addressed to:University Data Protection Officer

The University of Winchester
Winchester SO22 4NR

Tel: +44 (0)1962 841515
Fax: +44 (0)1962 842280

Copies of the University's full policy on Data protection are available from the Data Protection Officer on request.

Data Protection Act Register of personal data processing

Please complete the form as fully as possible. It is essential that we have a complete record of all personal data processing within The University of Winchester. Personal data means information about living individuals, regardless of the method of processing - it could be on computer, in filing cabinets or card index files. Some note books will also be covered. Include all work data held at home. It may be the information you access is also accessible by others within the department - please still list. Please duplicate this sheet if more space is required.

Your name..... **Your department/Faculty.....**

Ref	**Type**: Manual (M) Computer (C)	**Location:** - where file and/or database is found	**Data Subjects:** - type of people whose details are held e.g. student, staff,	**Data Class:** - describe info. held e.g. name & address	**Purpose:** - reasons why information is being held	**Sources:** - where or who is the data obtained from	**Disclosures**: - who else sees or receives the information - include other departments	**Retention Period**	**Justified?**

Please return this form to: **Ext No:** **Email:** **By: not later than (date)**

☐ For admin use