# Data protection - Code of Practice

*Set out below is the University's code of practice on data protection, which accords with the Data Protection Act and takes into account the codes of practice published periodically by the Office of the Information Commissioner.*

*The code falls into two sections. The first, covered in paragraphs 1-49, constitutes a statement of general policy, which includes an indication of the University's obligations under the Act. The second section, covered in paragraphs 50-66, provides brief guidance notes for staff in connection with handling personal data.*

## POLICY

### Introduction

1. The University needs to process certain information about its employees, students and other individuals, examples of which are set out in paragraph 6 below and in Appendix I to this code of practice. In so doing, the University must comply with the Data Protection Act 1998 [the Act]. The Act contains eight basic principles, which state that personal data must:

    - be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
    - be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
    - be adequate, relevant and not excessive for those purposes
    - be accurate and kept up to date
    - not be kept for longer than is necessary for that purpose (see paragraph 15 and Appendix II to this code of practice)
    - be processed in accordance with the data subject's rights
    - be kept safe from unauthorised access, accidental loss or destruction
    - not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

2. Some of the notable features of the Act are that:

- it places restrictions on what the University can do with personal data ; certain conditions, which include obtaining data subject consent (1), must be met before processing can take place. The term 'processing' covers almost anything that is done to data by reference to individuals and the practical implications of these restrictions are wide-ranging
- the right of access for staff and students to personal data that relate to them

(There is no entitlement to immediate or on-site access but the Act places a responsibility on the University to respond to access requests in good time (2); to this end, all data subject access requests will be handled centrally (see paragraphs 16-17 below).)

- It places an emphasis on data security, especially in relation to the unauthorised disclosure of personal data to third parties.

3. The University and all staff or others who process or use any personal information must ensure that the data protection principles and the law under the Act are followed and fully implemented. In order to facilitate this, the University has developed a code of practice on data protection. The references to personal data made within this document apply to data held within the University on any living individual, not just students and staff.

**Status of the Policy**

4. This policy forms part of the formal contract of employment for staff and part of the formal agreement between students and the University. Staff, and where appropriate students, must abide by this policy and any failure to comply with the code could result in disciplinary proceedings.

5. Those with honorary contracts or 'Visitor' status - for example, members of NHS staff who teach University students and Visiting Professors and Fellows - will also be expected to comply with this policy insofar as they come into contact with personal data through the University and in connection with the provision of their own personal data.

**What are personal data?**

6. Personal data means information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which the University has or may have in the future. This includes names and addresses, features such as hair and eye colour - which will often be in the form of photographs - student attendance records and marks, ethnic origin, qualifications and experience, details about staff sick and annual leave, dates of birth or marital status. Furthermore, any recorded opinions about or intentions regarding a person are also personal data; and this includes both student progress reports and staff review reports.

7. The Act covers ALL personal data processed by the University, irrespective of whether these are held by individual members of staff in their own separate files (including those held outside the University campus) or in departmental or faculty records systems or at the centre of the University.

8. The Act distinguishes between ordinary personal data such as name, address and telephone number and sensitive personal data relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive data is subject to much stricter conditions. In particular, processing of sensitive data requires explicit consent. While the Act permits the processing of data without consent where this is for the legitimate activities of an institution and is not to the detriment of individuals, in most instances consent to process ordinary and sensitive data is obtained routinely by the University for the avoidance of doubt (see paragraphs 12-14 below and Appendix I).

**Electronic and manual data**

9. As a public body all personal data, whether held in electronic or manual form, is generally covered by the Act.

10. Personal data within emails, letters, handwritten notes and even tape recordings are covered.

11. In practical terms, it seems prudent to assume anything recorded relating to an individual may fall under the provisions of the Act.

**Subject Consent**

12. In many cases, the University can process personal data only with the consent of the individual. In some cases, if the data are sensitive, explicit consent must be obtained. The University has a duty, under certain circumstances, to ensure that staff are suitable for the job, and students for the courses offered. On occasion, checks will be made with the Disclosure and Barring Service. (There are, for example, some jobs or courses which will bring the applicants into contact with children.) Where this is relevant to the job, the University may also ask for information about particular health circumstances.

13. As noted in paragraph 8 above, in most instances staff - and where appropriate, students - will not need to consider whether consent is required or to obtain consent to process from data subjects because such consent is obtained routinely by the University. All applicants for employment or for student places are asked to signify their consent to the University processing both ordinary and sensitive personal data on application for the purposes of processing that application. Upon student registration or acceptance of an offer of employment, students and staff are asked to give consent to processing a wider range of data. Agreement to the University processing these personal data is a condition of acceptance of a student onto any course and a condition of employment for staff; a refusal to provide consent may result in discontinuance of the application. Further information on this point is set out in Appendix I to this code of practice.

14. Consent to process the personal data of external inquirers or other users of the University's services will be unnecessary in most instances as the University can rely on the provision within the Act for processing without consent for legitimate and non-prejudicial purposes (see footnote 1). However, if personal data relating to external individuals is to be used subsequently for purposes other than the original enquiry (for example, in creating a database to be used in advising individuals about the University's services) consent should be obtained as a precaution. (See paragraph 53 below for guidance)

**Retention of Data**

15. It is not in the interest either of data subjects or of the University to retain unnecessary or duplicative information. The University does, however, retain some data relating to

former staff and students - most of which is held either in the Central Records Office or the University Archive - partly in order to comply with statutory requirements but also as a way of maintaining a complete historical record. Nonetheless, it is University policy to discourage the retention of personal data within files for longer than it is needed. Guidelines for the retention of personal data are set out in Appendix II to this code of practice; and files forwarded to Central Records Office or to the Archive should be 'weeded' beforehand in accordance with this guidance.

**Access to data**

16. Subject to certain exemptions, staff, students and others in contact with the University will on most occasions have the right to access personal data that is being kept about (3). This will normally be provided in the form of copies of the personal data or a report of the data held, depending on the type and format of the original data. Any person who wishes to exercise this right should complete the University's Subject Access Request Form (see the Request form for access to personal information) and forward it to Adrian Slater (Secretariat) with the required proof of identity. The University will levy a charge of £10 on each occasion that access is requested. It is illegal to dispose of personal data relating to an individual once he or she has lodged a written subject access request and paid the relevant fee.

17. The University aims to comply with requests for access to personal information from data subjects as quickly as possible, but will ensure that it is provided within 40 days from the date of the request.

**Staff obligations**

18. Staff may have responsibilities for processing personal data about students or colleagues, and are also data subjects in their own right. In connection with personal data on students and colleagues, all staff must comply with University guidelines on data protection. The University cannot carry out its legal responsibility to maintain up-to-date personal data unless staff:

    - ensure that any information that they provide to the University in connection with their employment is accurate and up to date
    - inform Human Resources or their department as appropriate about any changes for which they are responsible, for example, changes of address (the University cannot

be held accountable for errors arising from changes about which it has not been informed) .

19. Staff who supervise students who come into contact with personal data for the purposes of study or research are responsible for drawing their attention to this Code of Practice.

20. Inevitably, there will be occasions when personal data will be transferred from one area of the University to other. Where this occurs, the transfer must be reasonable and legitimate (taking into account the reasons for its initial collection). Furthermore, staff receiving or transferring sensitive data must be mindful of the need to maintain confidentiality.

**Student obligations**

21. Students must ensure that all personal data provided to the University are accurate and up to date. They must ensure that any changes, of address, for example, are notified to the Student Office, to their parent department and to other offices as appropriate (the University cannot be held accountable for errors arising from changes about which it has not been informed).

22. For the avoidance of doubt it is emphasised that students who come into contact with personal data through the University - for the purposes of research or study, in pursuit of an academic qualification and under the direct supervision of a member of staff - will be covered by the University's notification to the Information Commissioner. In such cases, staff must notify students about - and students must abide by - the relevant provisions of the code of practice (and see in particular paragraphs 38-40). The University is not responsible for notification of personal data processed by students for their own use.

**Data Security**

23. All staff (and where appropriate, students) must adhere to University policy and guidelines on data security, including the University's Information Protection Policy. Generally, staff and students must ensure that:

    - any personal data which they hold are kept securely

- personal information is not disclosed either orally or in writing, or in any other way, intentionally or otherwise to any unauthorised third party .

24. Staff should note that unauthorised disclosure may be a disciplinary matter, and could be considered gross misconduct in certain cases. (Guidance on authorised disclosure is set out in paragraphs 56-59 below.)

25. Additionally, staff must ensure that, where a data processor processes data on the University's behalf (a mailing agency, for example) there is a written contract between the parties which specifies that the processor agrees to act on the University's instructions and to abide by the provisions of the Act in connection with data security. Further guidance on appropriate terms for such a contract can be obtained from Adrian Slater, the University's Legal Adviser.

26. Staff should make reasonable efforts to ensure that all personal information is kept securely but should pay particular attention to the security of sensitive data. All personal data should be accessible only by those who need to use it and sensitive data must be either:

    - kept in a lockable room with controlled access, or
    - kept in a locked filing cabinet, or
    - kept in a locked drawer, or
    - protected by password, if held on a computer, or
    - kept only on disks which are themselves kept securely .

27. While the security of the campus network is the responsibility of the University, individuals will need to take appropriate security precautions in respect of day-to-day PC usage. Care must be taken to ensure that data on the screens of PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where they can be accessed by unauthorised staff. When manual records are no longer required, they should be shredded or bagged and disposed of securely; and the hard drives of redundant PCs should be wiped clean (a procedure that is already standard practice in ISS).

28. Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the

off-site use of personal data is similarly increased. For these reasons, staff (and where applicable, students):

- should take personal data off-site only when absolutely necessary, and for the shortest possible time, especially where sensitive data is to be processed
- should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside the University
- should also be aware that this code of practice and their responsibilities under it apply when data are processed off-site.

**Publication of University Information**

29. It is the University's policy to make as much information public as possible; in particular the following information may be available publicly:

- lists of staff
- names and work contact information of staff
- University e-mail addresses
- photographs of staff
- student pass lists.

30. It is of course a condition of employment or registration respectively that staff and students consent to the processing of their personal data (see paragraph 13 above). Nonetheless, it is recognised that there might be occasions when a member of staff or student has good reason for wishing details in certain of these lists or categories (or indeed, any other personal data) to remain confidential or to be restricted to internal access, in which case they should contact one of the designated data controllers (see also paragraph 47 below). It is understood that this is especially the case in connection with the publication of photographic images of staff and students, particularly on web pages; and such images should not be made publicly accessible without the consent of the individuals concerned.

**Monitoring of communications and use of CCTV (4)**

31. The University must ensure that its resources are not abused or used illegally, for example, for accessing pornographic material on the World Wide Web. In particular, both staff and students have responsibilities for using IT resources in accordance with

ISS codes and regulations. The University may from time to time monitor staff and student communications without giving notice; random monitoring of personal computer usage, however, will apply only to publicly-accessible computer clusters; and random monitoring of telephone calls will not take place.

32. In any case:

- any monitoring will be carried out only by a limited number of staff
- personal data obtained during monitoring will be discarded as soon as possible after the investigation is complete
- staff involved in monitoring will maintain confidentiality in respect of personal data.

33. For reasons of personal security, to protect University premises and the property of students and staff, and to ensure that the University's resources are not abused, closed circuit television cameras are in operation in certain campus locations. There are occasions when, to ensure the effectiveness of this surveillance, the presence of these cameras may not be obvious.

34. Students or staff who consider that the positioning of a closed circuit television camera or use of a webcam is inappropriate should contact either of the two designated data controllers (see paragraph 47 below).

35. A number of areas of the University may quite legitimately use webcams (for teaching purposes, and monitoring queues, for example). However, careful thought should be given to potential problems arising from the transfer of images of individuals (which are personal data) that potentially may be transmitted worldwide. In such circumstances, consent should be obtained from individuals or an appropriate warning sign should be posted within the area covered by the webcam

**World Wide Web and Email**

36. The provisions of the Act apply as much to web sites and to email as they do to data processing by any other means; any personal data downloaded from the web, included within a web site, or contained within an email are subject to the same restrictions as information held in manual files or on databases. In particular:

- those sending emails that include personal data on third parties should be confident that confidence and security will not be breached by the recipient, and they may wish to consider the use of encryption or other security measures
- authors of web pages should be aware that information posted onto a web page is potentially accessible worldwide (unless access is restricted in some way) - the type of data placed onto web pages should reflect this those setting-up a web page or site which involves processing personal data - including the creation of mailing lists - should seek consent to process such data (advice on which is available from Adrian Slater ) and should also include a privacy statement (advice on which is available within the University's Privacy Statement).

**Cross-border data flows**

37. The new Act places restrictions on the transfer of personal data outside the European Economic Area (EEA) (5), unless the country or territory involved ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. If, after careful consideration, it is regarded as essential that the transfer of personal data outside the EEA should take place - and if the transfer does not qualify as one of the circumstances when this principle does not apply - the consent of the data subject must be sought. Members of staff should note that this restriction has particular implications for international research projects and information placed onto web sites (see also paragraph 36 above).

**Research data**

38. Personal data processed only for research purposes receive certain exemptions where the data are not processed to support measures or decisions with respect to individuals, and where no substantial harm or distress is caused. In essence, such personal data:

- can be processed for purposes other than that for which they were originally obtained
- can be held indefinitely
- are exempt from the data subject right of access where the data is processed for research purposes and the results are anonymised.

39. The Act does not give blanket exemption from all data protection principles for data provided and/or used for research purposes. Most of the principles apply (notably the requirement to keep data secure); and staff will need to assess the legality of processing on each occasion that data are provided for research purposes (see paragraph 60 below (6)). Furthermore, researchers will need to ensure that:

- data subjects whose personal data will be used in research are advised as to why the data are being collected and the purposes for which it will be used
- a suitable mechanism is in place to ensure that data subjects can meaningfully exercise their right to object to the processing of their data on the grounds that it would cause them significant damage or distress
- particular care is taken when the processing involves sensitive personal data (see paragraph 8 above) for which stricter conditions apply, including the need to obtain explicit consent for processing .

40. Finally, those conducting research involving the processing of personal data should do so in the context of any ethical guidelines or codes of practice particular to their field of study; and it may be necessary to confirm the compatibility of such codes with the Act.

**Confidential references**

41. For practical purposes staff must assume that we can no longer guarantee confidentiality in respect of references received by the University or expect that those we provide will remain confidential. Advice on the phrasing of a clause suitable for inclusion in written correspondence requesting a reference (making clear the University's inability to guarantee confidentiality) is available from Adrian Slater.

**Disclosure of references**

42. Where a data subject access request is lodged by an individual, the University will need either to obtain consent to disclose any references covered by the request or to disclose references in anonymous format.

**Provision of references overseas**

43. Explicit consent must always be sought from the data subject where references are provided for organisations located outside the EEA (see paragraph 37 above).

**Examination Marks**

44. Students will be entitled to information about examination marks. However, there is provision under the Act for this to take longer than other information to provide. (The University may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the University, but may not withhold marks for these reasons.)

45. Internal and external examiner comments, whether made on the script or in another form that allows them to be held and applied to the original script or to a specific candidate (e.g. an examiner's report) are covered by the Act. A data subject has the right to request that a copy or summary of such data is provided within the stipulated timescale 'in an intelligible form'. This implies that examiner's comments on scripts and assessed work should be capable of being produced for a data subject in a meaningful form and that they should be both intelligible and appropriate.

46. The long-established practice of publishing student pass lists on departmental noticeboards is regarded as acceptable to the Information Commissioner provided that they do not include details that would allow individual students to be contacted (through the inclusion of telephone numbers or email and postal addresses, for example). The rights of an individual student who does not wish his or her name to be included on the list should, however, be respected and their name withdrawn.

**Complaints**

47. Any member of staff or student:

- who wishes to raise a concern or complaint regarding the processing of his or her personal data should contact the designated data controller in order to discuss the options for resolving their concerns;
- who considers that the policy has not been followed in respect of personal data should raise the matter with the University's designated data controller. If the matter is not resolved with the help of the data controller it should be raised under the appropriate grievance or complaints procedures (7).

**Conclusion**

48. Compliance with the 1998 Act is the responsibility of all members of the University. Any breach of the data protection policy may lead to disciplinary action being taken, or access to University facilities being withdrawn, or even a criminal prosecution by third parties. Any questions or concerns about the interpretation or operation of this policy should be taken up with one of the University's designated data controllers.

**Further information**

49. Data protection is a complex area and in addition to the brief guidance notes set out below, further information is available to staff from the following sources:

    - the University's designated data controller: Adrian Slater, the University's Legal Adviser (on 34079 and email a.j.slater@leeds.ac.uk) •- departmental/faculty data protection advisers
    - internal training courses.

**Guidance Notes for Staff**

50. In addition to any responsibilities for processing personal data about students, staff applicants or other individuals, staff are also data subjects in their own right. Many staff process personal data about students on a regular basis, when marking registers, or assessments, writing reports or references, as part of a pastoral or academic supervisory role, or in connection with the student administration, including registration, fees, grants, awards, prizes and matters connected with academic appeals and student discipline. Some staff frequently also process information about other staff, especially in the context of recruitment and internal procedures, including those for promotion, disciplinary matters and appeals. Some staff also process data about individuals who are not staff, students or applicants.

51. The University ensures that all students give their consent to processing ordinary and sensitive personal data via registration procedures, and that they are notified of the categories of processing as required by the 1998 Act.

52. Consent to process ordinary and sensitive personal data has been sought from individual members of staff appointed from February 2001. Staff appointed before this date will be deemed to have given their consent.

53. Where - exceptionally - consent to process personal data needs to be sought from external individuals (see paragraph 14 above) the following brief phrases will suffice (with variations according to the type of data and its proposed use):

Enquiries made over the telephone or in person:
"May we assume that you are content for the University to use your personal data (by which we mean your name and address) to provide you with information about our services?"

Enquiries generating written correspondence:
'Unless you advise us to the contrary, we will assume that you are content for the University to use your personal data (by which we mean your name and address) to provide you with information about our services.'

54. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the University's Data Protection Policy. In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- fair;
- kept and disposed of safely, and in accordance with the University's policy .

55. All staff, including non-contracted staff, will be responsible for ensuring that data is kept securely.

56. Staff must not disclose personal data to a third party (9) unless:

- reasonable steps have been taken to verify the identity of the third party, and
- the type of data disclosed, and the party or parties to whom it is disclosed, are among those for which consent is sought routinely by the University (as set out in the sections on the use of personal data relating to staff and students in Appendix I to this code of practice ) , or

- if disclosure for such data is not sought routinely, the member of staff or student concerned has otherwise given consent to the disclosure, or
- disclosure is in the best interests of the student or member of staff, or is urgent and necessary in the circumstances, or is required in compliance with the law (and see paragraph 57 below) .

57. Third party disclosure under the final bullet point of the previous paragraph should occur only in very limited circumstances (for example, if personal data is required urgently where a member of staff or student is injured and unconscious, but in need of medical attention).

58. Where disclosure is requested by the police, the matter should be referred to Roger Gair, the Secretary to the University, (on 34011) or Adrian Slater (on 34079). Outside office hours, contact with these individuals should be made via the University's Security Service (35494 and 35495).

59. Where a member of staff is in doubt about how to proceed on third party disclosure, he or she should contact either the relevant departmental adviser or the University's data controller (or in their absence, a member of the University's security service).

**Staff Checklist for Processing Data**

60. Before processing any personal data, all staff should consider the checklist set out below.

- do you really need to record the information?
- is the information 'ordinary' or is it 'sensitive' (see paragraph 8 above)?
- does the University have the data subject's consent, i.e. is it included in the sections on the use of personal data relating to staff and students set out in Appendix I to the code of practice or has it been obtained in some other way ?
- are you authorised to collect/store/process the data?
- unless the data have been obtained from a reliable source, have you checked with the data subject that the data are accurate?
- are you sure that the data are secure?
- if you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member (or other data subject) to collect and retain the data?

**Access requests**

61. The Act gives individuals the right to access data held about them by the University. However, this is not an entitlement to immediate access - the University has forty days in which to comply with data subject access requests - and staff should forward all such requests to Adrian Slater in the Secretariat.

62. The Act also means that any recorded opinion about or intentions regarding a person are also personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (and this includes e-mails and audio recordings, in addition to computer and manual files) and when files are weeded for unnecessary or duplicative material. The following is a useful test to apply to 'doubtful' comments:

    - Is this comment fair, accurate and justifiable?
    - If I were to show this to the data subject, would I still be confident that the comment is fair, accurate and justifiable?

    If the answer to the questions - and in particular the first question - is 'No', then the comment should go unrecorded.

63. Access rights also mean that the confidentiality of references provided either internally or for external bodies can no longer be assumed. Again, this should be borne in mind when references are drawn up and in general terms the information provided in references should:

    - confirm the accuracy of or provide factual information
    - differentiate between statements of fact and opinion
    - express only justifiable opinions, based on first-hand experience
    - be fair and accurate
    - avoid ambiguous or coded language .

64. All staff should ensure that inappropriate data are neither recorded nor retained. Once a data subject has requested access, the law specifies that data relating to him or her must not be 'weeded'.

## Cross-border data flows

65. Staff must take especial care in connection with requests for the transfer of personal data outside the European Economic Area (EEA) (see paragraph 37 above). In particular, staff should not:

- disclose personal data requested by non-EEA governments, agencies and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without the specific and informed consent of the data subjects concerned
- disclose personal data requested by non-EEA governments for the purpose of determining liability to attend National Service, without the specific and informed consent of the data subjects concerned.

## Further information

66. Further information and advice is available either from your departmental data protection adviser or from the University's designated data controller, Adrian Slater (on 34079 and on email a.j.slater@leeds.ac.uk).

Footnotes:

(1) The Act does, however, permit the processing of data without consent where this is for the legitimate activities of an institution and is not to the detriment of individuals (see also paragraphs 14 and 19).

(2) Institutions have a maximum of 40 days in which to comply with a request for access by a data subject.

(3) This right will not for example, apply to documents regarded as being within the ambit of 'legal privilege', that is, those setting out legal counsel and related correspondence; and where access may disclose personal data relating to a third party who has not consented to such disclosure (in respect of confidential references, for example).

(4) The monitoring of communications and the use of CCTV fall within the ambit of the Act because they invariably involve the processing of personal data in some form.

(5) The European Economic Area consists of the fifteen EU Member States together with Iceland, Liechtenstein and Norway .

(6) Further information on this matter is provided in a document setting out frequently asked questions.

(7) Where there is uncertainty as to the appropriate procedure, this will be determined by the Secretary to the University.

(8) Following restructuring from 1 August 2003 , it is expected that - in the interests of efficiency and effective co-ordination - each faculty will wish to consolidate the roles of existing departmental data protection advisers into a single faculty adviser.

(9) Further information on who constitutes a third party is provided in a document setting out frequently asked questions.