JISC Data Protection Code of Practice for the HE and FE Sectors

INFORMATION
LAW & TECHNOLOGY UNIT

Part of the University of Hull Law School

Introduction to the Code of Practice

JISC Assist has commissioned Andrew Charlesworth, Director, Information Law and Technology Unit at the University of Hull, to prepare a Code of Practice on the Data Protection Act for the Further and Higher education communities. General principles of the Act are not covered, as they are widely available elsewhere; the Code of Practice concentrates on the key issues for the HE and FE sectors.

It should be noted that the Code of Practice is not intended to be mandatory or prescriptive, but are a guide to best practice in this area. Nor, of course, can compliance with the guidelines guarantee compliance with the law.

JISC is pleased to present version one of this Code of Practice as advice for the current year. The Codes of Practice will be reviewed as experience of the Act in operation is gained, further updates will made available via the JISC web site http://www.jisc.ac.uk/.
One example of their application can be found at University of Lancaster HEFCE Good Management Practice Project on Data Protection and Personal Data. The web site will be developed for this project and will be hosted at http://www.lancs.ac.uk/dataprotection

It should also be noted that the new JISC Legal Information Service will make resources available on the operation of the Act. Further announcements about this new service will be made via the JISC web site, and on JISC-ANNOUNCE@mailbase.ac.uk.

Other relevant publications available at http://www.jisc.ac.uk/pub/index.html:

- Senior Management Briefing Paper no.9.The Data Protection Act 1998, which deals with the broad Data Protection issues
- Senior Management Briefing Paper no.10.New Developments in UK Internet Law

We hope that this Code of Practice will assist institutions in their compliance with the 1998 Data Protection Act and would welcome feedback and comments as part of the review process. These should be sent to JISC Assist:

Contact JISC Assist via e-mail at:
assist@jisc.ac.uk

Or telephone JISC Assist on:
0117 954 6850

CONTENTS

Foreword and Acknowledgements 4
Speakers 4
Administration 4
Comments, Advice and Information 4
Introduction 5
Use of Personal Data by Employees 6
Personal data processed under an institutional notification 6
Personal data processed outside an institutional notification 6
Employee access to, and use of, Personal Data 6
Student Use of Personal Data 8
Personal data processed under the effective control of an institution 8
Personal data processed outside the effective control of an institution 8
Student access to, and use of, Personal Data 8
Transfer of Data to Third Parties 10
Security of Personal Data 13
Institutional Framework for Data Security 13
Employees and Student Security Training and Management 15
Vendors, Contractors, and Suppliers 16
Transfer of personal data 16
Migration or upgrade plans 16
Back-up of personal data 17
Employee and student use of personal data off-site, on home computers, or at remote sites 17
Disposal of Data 18
Examinations 19
The Examination and Assessment Process 19
Examination scripts 19
Internal Examiners' comments 19
External Examiner's comments 20
Automatic processing 20
Examination Board Minutes and related documentation 20
Disclosure of results 21
Use of Personal Data in Research 22
Confidential References 23
References given by HE and FE institutions 23
References received by HE and FE institutions 23
References internal to HE and FE institutions 24
Transfers of Personal Data to non-EEA Countries 25
The Internet and World Wide Web 27
General Institutional Webpages 27
Institutional Staff and Student Directories 28
Web pages used to collect personal data 28
Personal employee and student webpages on institutional machines 29
Internet and Intranet Monitoring 29
Collection and Processing of Personal Data relating to Disability 32
Counselling Services 33
Careers Services 35
Other Information 36
Next of Kin/Emergency Contact Information 36
Applications for Access Funding and other discretionary funding 36
Alumni Records 37
CCTV and similar surveillance equipment 37
Retention of Records containing Personal Data 38

Foreword and Acknowledgements

This Code of Practice for the Higher and Further Education Sectors on the Data Protection Act 1998 (referred to throughout as the 1998 Act) is the outcome of four Workshops, funded by JISC Assist, that were held in London, Loughborough, Edinburgh and Cardiff during February – April 2000. These Workshops were an opportunity for those tasked with implementing the Act in HE and FE institutions to meet and discuss the implications of the 1998 Act, identify particular problem areas in the HE and FE sectors, and to compare strategies for their institutions. The Workshops thus served an educational role, but their primary purpose was to provide a clear understanding of the issues that would need to be addressed in this Code of Practice.

Speakers

The speakers at the Workshops were:

- Andrew Charlesworth, Director, Information Law and Technology Unit, University of Hull
- Rosemary Jay, Senior Consultant, Masons Solicitors
- Lucy Inger, Senior Associate, Masons Solicitors
- Linda Malloy, Associate, Masons Solicitors
- Adrian Tribe, Web Editor, Birkbeck College, University of London
- Dr Trevor Field, Senior Assistant Secretary, University of Aberdeen

Administration

JISC Assist provided the administration for the Workshops and particular thanks should go to Jane Williams, Ann Hughes, Amber Thomas, Jane Charlton, Clare Rogers & Shirleen Craig.

Comments, Advice and Information

The Mailbase e-mail discussion list <Data-protection@mailbase.ac.uk> was an invaluable aid to enabling feedback on the various drafts of this Code of Practice and thanks must go to the listowner, Sally Justice, Data Protection Officer and Webmaster at South Bank University. Space constraints mean that it is not possible to thank individually all those who offered valuable comments and advice but special thanks should go to:

- Dr Trevor Field, Senior Assistant Secretary, University of Aberdeen
- John Hitches, Data Protection Officer and Information Security Officer, Kingston University.
- Anne Johnson, Assistant Registrar, University of Sussex
- Dr John M Gledhill, Academic Registrar, Coventry University
- Andrew Cormack, Head of CERT, UKERNA
- Maurice Frankel, Campaign for Freedom of Information
- Anne Kipling, Information Security Officer, Oxford Brookes University

As always in these circumstances, where one individual is tasked to pull a wide range of views, and opinions ideas, comments and advice into some kind of shape, the author is obliged to add that any infelicities of style and content remain, of course, his own.

Andrew Charlesworth - Senior Lecturer in IT Law & Director, Information Law and Technology Unit, University of Hull.

Introduction

The following Code of Practice is designed to provide guidance to the HE and FE sectors on issues of specific relevance to their day-to-day operations. As such, the Code of Practice does not provide an in-depth examination of the general principles of the Data Protection Act 1998, which are widely available elsewhere, but concentrates on key issues of concern raised at the JISC Data Protection Workshops. Where guidance notes for specific aspects of the handling of personal data are available from the Office of the Data Protection Commissioner (ODPC), as is the case with Closed Circuit Television (CCTV), this Code of Practice will refer readers to them.

It should be noted that the Code of Practice is a guide to best practice in this area, and is not designed to be mandatory or prescriptive in nature. HE and FE institutions may thus decide to adopt data protection practices that differ from those suggested here according to their particular circumstances.

Use of Personal Data by Employees

Personal data processed under an institutional notification

Where employees at HE and FE institutions are processing personal data within their institution, as a legitimate part of their employment (e.g. research, teaching, consultancy and administration), they should be able to rely upon the notification to the Data Protection Commissioner (DPC) provided by their institution.

HE and FE institutions should ensure that their institutional notification adequately covers the legitimate data processing activities of their employees.

HE and FE institutions should:

- consult the notification template for HE and FE institutions provided by the Data Protection Commissioner for guidance on best notification practice;
- audit their institutional personal data processing activities on an annual basis to ensure that these match the activities that have been notified.

Personal data processed outside an institutional notification

Where employees process personal data within their institution for purposes unconnected with their employment such processing may be deemed to be:

- for their own personal or domestic purposes. Such processing will be exempt from notification.
- for other purposes, such as commercial exploitation of personal data unrelated to the institutional notification. Such processing may require notification to the DPC.

HE and FE institutions are not responsible for notification of personal data processed by employees for purposes unconnected with their employment e.g. for their own personal or domestic purposes.

HE and FE institutions should ensure that employees are provided with guidelines explaining the need for notification where their processing is likely to fall outside the institutional notification or the "personal or domestic purposes" exemption.

HE and FE institutions should consider:

- whether employees should be permitted to process personal data using institutional resources where such processing is for purposes unconnected with their employment
- the terms and conditions under which such processing should be permitted, if it is allowed.

Employee access to, and use of, Personal Data

Employees will often be expected to collect, hold, and process personal data as part of their employment duties. It is important to ensure that employees are apprised of the rights of data subjects, and respective employer and employee responsibilities with regard to access to, and use of, personal data. This is particularly so where employees may be processing sensitive personal data in the course of their employment.

HE and FE institutions should ensure that employees are:

- aware that all personal data collected, held, and processed on institutional machinery, including via WWW tools and other Internet software are subject to the Data Protection Principles
- aware that all personal data collected, held, and processed in structured manual files within institutions are subject to the Data Protection Principles
- aware of the circumstances under which employees may legitimately access, process and disclose personal data held on institutional computer systems in the course of their employment.

HE and FE institutions should ensure that:

- guidelines for the proper use of personal data within an institution are available to all employees
- there is a mechanism to ensure that misuse of personal data by employees within an institution can be identified and remedied
- there is a mechanism for data subjects to object to the accessing, processing and disclosure of their personal data held by employees within an institution, in structured manual files or computerised form, where data subjects feel that such use may cause them significant damage or distress

Student Use of Personal Data

Personal data processed under the effective control of an institution

In cases where students are processing personal data within HE and FE institutions (e.g. on institutional machinery):

- for the purposes of research or study;
- in pursuit of an academic qualification;
- and under the direct supervision of a member of staff,

If those HE and FE institutions can demonstrate direct and effective control over the personal data then the students conducting the research, or engaged in the course of study, can rely upon the notification to the DPC provided by their institutions.

HE and FE institutions should ensure that personal data processed for research and study purposes is adequately covered by their institutional notification.

Personal data processed outside the effective control of an institution

Where students process personal data, and that processing is:

- for the purposes of research or study in pursuit of an academic qualification, but not under the direct supervision of a member of staff; or
- their institutions cannot guarantee direct and effective control over the personal data;

such processing will be deemed to be for the student's own personal or domestic purposes and the processing will be exempt from notification.

HE and FE institutions are not responsible for notification of personal data processed by students outside the effective control of those institutions e.g for students' own personal or domestic purposes.

Where students process personal data, and that processing is:

- not for the purposes of research or study in pursuit of an academic qualification; or
- for the purposes of research or study in pursuit of an academic qualification but with a view to the students commercially exploiting its products

notification by the students to the DPC may be required.

HE and FE institutions should ensure that students are provided with guidelines explaining the need for notification where their processing is likely to fall outside the institutional notification or the "personal or domestic purposes" exemption, e.g. where the processing is intended to lead to the commercial exploitation of personal data.

Student access to, and use of, Personal Data

Students may on occasion be in a position to access personal data held and processed within HE and FE institutions. It is important to ensure that students are apprised of the rights of data subjects, and both their, and their institution's, responsibilities with regard to access to, and use of, personal data. This is particularly so where students will be processing personal data in the course of their studies.

HE and FE institutions should ensure that students are:

- aware that all personal data collected, held, and processed on institutional machinery, including via WWW tools and other Internet software are subject to the Data Protection Principles
- aware that all personal data collected, held, and processed in structured manual files within institutions are subject to the Data Protection Principles
- aware of the circumstances under which they may legitimately access, process and disclose personal data held on institutional computer systems

HE and FE institutions should ensure that

- guidelines for the proper use of personal data within an institution are available to all students
- there is a mechanism to ensure that misuse of personal data by students within an institution can be identified and remedied
- there is a mechanism for data subjects to object to the accessing, processing and disclosure of their personal data held by students within an institution, in structured manual files or computerised form, where data subjects feel it may cause them significant damage or distress

HE and FE institutions should consider:

- whether students should be permitted to process personal data using institutional resources where such processing is for purposes unconnected with their studies
- the terms and conditions under which such processing should be permitted, if it is allowed.

Transfer of Data to Third Parties

HE and FE institutions collect a wide range of personal data relating to staff and students for the institutions' own purposes, and to meet external obligations. Both these types of collection by institutions may result in the eventual transfer of personal data to third parties. The 1998 Act aims to provide data subjects with a greater degree of control over the parties to whom their personal data is released. Institutions must therefore ensure that any transfers of personal data that they engage in are permitted under the 1998 Act.

Transfers will be permitted where data subjects 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 institution requests that consent be given by the data subject in order that the institution can provide personal data to a third party, and no communication from the data subject is forthcoming, the institution must infer that consent is withheld.

The institution must ensure that personal data under its control is not disclosed to unauthorised third parties. Unauthorised third parties include:

- A person or organisation to whom the data subject has not consented that the data be disclosed;
- 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.

"Unauthorised third parties" will include family members, friends, local authorities, government bodies, and the police, unless non-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 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.

Data may also be disclosed to third parties without consent where:

- it is to be used for research purposes, subject to the rules relating to use of personal data in research (see below);
- it is information which the institution is obliged by legislation to provide to the public, by publishing it, making it available for inspection, or by other means, for free or for a fee;

- where the disclosure is required by legislation, by any rule of law or by the order of a court (i.e. HE and FE institutions' are legally obliged by the Higher Education Statistics Agency to collect first destination data for graduating students).

Transfer of data to third parties outside the European Economic Area will require the application of further DP rules, and such transfers are discussed below.

HE and FE institutions should ensure that:

- their staff and students are aware that, as data controllers, institutions owe an obligation to data subjects not to pass on their personal data to third parties, which may only be waived by consent, or in exceptional circumstances.
- at the time that their personal data is collected, data subjects are informed about the recipients (or classes of recipients) to which that information will, or may be, disclosed, and the reasons for that disclosure.
- where an employee requests personal data about another data subject within the institution, such information should be released only if, and only to the extent that, the member of staff requires the information in order to perform his or her official duties.
- the legal restrictions upon an institution's ability to disclose personal data to third parties are communicated clearly to parents, relatives and guardians of staff and students when requests for personal data are made.
- reasonable measures are in place to prevent the inadvertent disclosure of personal data (i.e. a student's attendance at a particular institution) to unauthorised third parties. When staff receive enquiries as to whether a named person is a student of the institution, 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.
- enquiries from Embassies and High Commissions are treated with extreme caution. Data subjects may choose to have little or no contact with representatives of their home states, the extent of the relationship is a matter for the data subject, not the institution, to determine.
- if a request for information about a data subject is refused, but the subject-matter of the enquiry is evidently of importance to the data subject, they should be informed of the enquiry. This will allow the data subject to contact the enquirer should they so wish.

HE and FE institutions may wish to consider advising staff that:

- where a request for information is received by telephone from an enquirer who appears to be a person to whom information may properly be disclosed, it is good practice to offer to telephone back with the information to ensure some measure of authentication.
- as an alternative to divulging personal data, an institution will 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.
- where the matter is urgent, an attempt should be made to contact the student by telephone or other means in order to put him or her in touch with the enquirer.

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 be required:

- to provide reasonable proof of their personal identity and organisational affiliation according to the circumstances of the request and the nature of the personal data requested;
- to conform to any procedural or documentary requirements imposed by the institution or by the requesting organisation (i.e. an institution might require that all requests for personal data on staff or students be made via the institution's data protection officer, and that requests for personal data by police officers should be supported by warrant, or by suitable paperwork provided by the local force stating that the information is required in support of an ongoing investigation).
- where reasonable, to provide a written and signed document to the institution containing: the purpose for which the data is being requested; the time for which it is to be held; and a warranty that it will be held and processed in conformity with the Data Protection Principles.

Security of Personal Data

Institutional Framework for Data Security

A data subject may apply to the court for compensation if he/she has suffered damage (financial loss or physical injury, and possibly associated distress) because personal data have been lost or destroyed or disclosed without the authority of the data user, or access has been obtained to personal data without the authority of the user. A court dealing with a claim for compensation will need to consider if the institution has taken all reasonable care to prevent the particular loss, destruction, disclosure or access.

HE and FE institutions are obliged under the 1998 Act to have in place an institutional framework designed to ensure the security of all personal data during the collection to destruction cycle. A key current international benchmark for Information Security Management Systems (ISMS) is BS7799. A framework that meets this standard will provide a high level of compliance with the 1998 Act. Where complete compliance with BS7799 is infeasible or unreasonable for all, or certain types of, institutional personal data processing operations, certain minimum standards should still be met. Such standards should ensure:

- a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
- that data security is assured no matter where or by whom data is stored or processed and throughout the whole procedure, including the transmission of data.
- that there are clear lines of responsibility and the controller's ultimate responsibility for data security is clearly understood.

HE and FE institutions should consider:

- the extent to which their personal data holdings are computerised or manual, and whether existing computerised and manual systems duplicate certain types of personal data;
- the extent to which their personal data holdings are distributed around their site(s), and how this distribution affects the management and security of such holdings, particularly of manual holdings;
- the continuing desirability of manual storage of personal data, given the difficulties of ensuring viable backup, security, and management systems in paper or microfiche holdings.
- the desirability and feasibility of computerised systems where data are de-personalized, or coded, or encrypted, with a secure key.

HE and FE institutions should, as a minimum, ensure that:

- existing and proposed personal data processing operations are evaluated for potential risks in order to determine the cost, effectiveness and practicability of proposed levels of security.
- appropriate levels of security are applied, commensurate with the anticipated risks, and appropriate to the type of personal data held.
- agreed levels of security are applied, monitored and regularly reported upon as regards their effectiveness

- all staff are trained to take effective action to protect personal safety, data and equipment (in that order) in the event of disaster.
- competent people are assigned to be responsible for the accuracy and integrity of personal data held in each part of an institution's personal data processing operations.

Employees and Student Security Training and Management

A primary part of any HE or FE institution's personal data security framework will be the effective training and management of its employees and students in necessary security procedures. A significant proportion of unauthorised disclosure of, and access to, personal data occurs because employees and students are unaware of, or fail to adhere to, existing institutional guidelines. The potential consequences under the 1998 Act for institutions of unauthorised disclosure of, and access to, personal data are such that it is essential to both develop an institutional awareness of data privacy rules, and to provide a verifiable mechanism for sanctions for breach of those rules.

HE and FE institutions should ensure that:

- employees and students dealing with personal data are aware of the purposes for which the data has been collected, including the parties to whom disclosure may legitimately be made, and are aware that disclosure may not be made to other parties, unless one of the exemptions in the Act applies.
- employees and students dealing with personal data have a formal point of contact within the institution, such as a Data Protection Officer, where they can refer requests for disclosure under one of the exemptions in the Act (e.g. law enforcement)
- employees and students dealing with personal data are aware that their access to personal data is for specified authorised purposes only. Institutional regulations should provide that access to personal data by employees and students for unauthorised purposes (e.g. browsing of personal data, whether on computer or in manual files) will be a disciplinary offence
- employees and students must apply and abide by any relevant security requirements contained in agreements with outside bodies who may furnish personal data for university research purposes.
- employees and students are aware that casual access to personal data by unauthorised persons (e.g. members of the general public having access to personal data via VDU screens or printouts, or in unlocked filing cabinets stored in corridors or in unlocked rooms), by act or omission, should not be permitted. Institutional regulations should provide that acts or omission that lead to unauthorised access or disclosure to unauthorised persons will be a disciplinary offence.
- reasonable access control mechanisms including, where appropriate, the use of passwords, encryption, compartmentalised access and access logs, are used to detect and prevent attempts to access computer files through terminals or computer networks without authorisation.
- reasonable access control mechanisms including, where appropriate, security locks, secure rooms, authorised keyholders, and access logs are used to monitor access to manual files to prevent unauthorised access.
- institutional regulations provide that failure to adhere to the correct use of applicable access control mechanisms will be a disciplinary offence.
- basic security steps are taken to ensure that building perimeters and internal sensitive areas are secure, and that the general public, unescorted visitors, and unauthorized personnel be restricted from areas where personal data is used.
- existing security controls are reviewed for improvement or modification and that awareness programs, as well as policy and guidelines be established to protect personal data.

Vendors, Contractors, and Suppliers

Vendors, contractors, and suppliers are often required to have access to areas in which personal data may be stored or processed. In certain circumstances, it may also be necessary to allow contractors access to personal data (e.g. computer engineers) in the course of maintenance or repair work.

HE and FE institutions should ensure that contractors are:

- Controlled, documented, and required to wear some form of identification;
- Restricted from unnecessary admittance to areas where personal data is held or processed;
- Required to sign nondisclosure agreements where access to personal data is unavoidable.

HE and FE institutions should ensure that vendors and suppliers are:

- Controlled, documented, and required to wear some form of identification;
- Escorted throughout the general premises by the person they are visiting;
- Restricted from unnecessary admittance to areas where personal data is held or processed.

Employees and students should be advised to challenge, or report to security, individuals without proper credentials found in areas where personal data is held or processed.

Transfer of personal data

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

HE and FE institutions should ensure that personal data is transferred under conditions of security commensurate with the anticipated risks, and appropriate to the type of personal data held

Migration or upgrade plans

Changes to an institution's hardware or software systems may result in personal data becoming inaccessible or unreadable due to incompatibility between data formats meaning that the institution cannot properly ensure the data's accuracy and integrity.

HE and FE institutions should ensure that:

- future migration or upgrade plans for institutional systems are documented to address the potential effect of hardware, software and operating system upgrades, or obsolescence, on personal data processing operations.

- successful data transfer tests of existing personal data to new systems or file formats are carried out before those systems go live, and old systems, including manual systems, are discarded

Back-up of personal data

Loss or destruction of personal data may have severe consequences for the operations of HE and FE institutions, in addition to their incurring liability to individuals who have suffered damage or distress as a result of the loss or destruction of their personal data. Disaster recovery plans are thus an essential part of any institutional data protection framework.

HE and FE institutions should ensure that:

- a workable disaster recovery mechanism is in place for all personal data processing operations where it would be reasonable, by virtue of the importance of the personal data, for such a mechanism to be implemented.
- there are provisions for frequent back-up or duplicate copies of all personal data produced in personal data processing operations at an institution to be made, and securely stored, in a location wholly separate from that of primary data source (e.g. off-site).
- there are designated personnel tasked with the responsibility of ensuring the recovery of personal data, and establishing its accuracy and integrity, within a reasonable time following any disaster.

Employee and student use of personal data off-site, on home computers, or at remote sites.

Off-site use of personal data in manual or computerised form by employees or students presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should thus be aware of both the institutional and the personal liability that may accrue from their off-site use of personal data.

Employees and students should take particular care when laptop computers or personal machines are used to process institutional personal data at home or in other locations (e.g. in public places, or on public transport) outside the institution.

Employees and students should be required to ensure that when processing institutional personal data at home or in other locations:

- they take reasonable precautions to ensure that the data is not accessed, disclosed or destroyed as a result of act or omission on their part.
- they ensure personal data held in manual form is stored as securely as possible, and ideally is locked away when not in use.
- they 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.
- they back up system hard drives to avoid loss of data.
- they report all computer security incidents including virus infections to the institution

Employees and students should be required to ensure that when using laptops to process personal data they:

- 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
- record the model number and serial number of each hardware component associated with the laptop and keep this information in a separate location
- notify the institution immediately in the event of loss or theft
- consider file or disk encryption where possible

Disposal of Data

The proper disposal of personal data should be the final element in an institutional framework designed to ensure the security of personal data. 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; paper and microfilm documentation containing sensitive personal data should be horizontally and vertically shredded or incinerated. 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.

HE and FE institutions should ensure that:

- all paper or microfilm documentation containing personal data is permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
- all computer equipment or media to be sold or scrapped have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.
- employees and students are provided with guidance as to the correct mechanisms for disposal of different types of personal data and regular audits should be carried out to ensure that this guidance is adhered to. In particular, employees and students should be made aware that erasing electronic files does not equate to destroying them.

Where disposal of equipment or media is contracted to a third party, institutions should ensure that the contract contains a term requiring the third party to ensure that all personal data is completely destroyed, and permitting the institution to audit the third party's performance of that term at regular intervals.

Examinations

The Examination and Assessment Process

The 1998 Act states that "new processing" which started after 24 October 1998 is immediately subject to the new legislation, whereas processing which was under way before that date will be subject to the transitional arrangements. "Processing" refers to purposes and procedures - thus, the addition of data to an existing database would not count as new processing. In the case of examinations and actual scripts, the continuation of previous practices, applied to new students, will also not count as new processing until the end of the transitional period.

HE and FE institutions should assume that, 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.

Examination scripts

Examination scripts are expressly exempted from the data subject access rules. This means that HE and FE institutions are under no obligation to permit examination candidates to have access to either original scripts or copies of the scripts.

HE and FE institutions have the absolute discretion to deny subject access requests for examination scripts. "Examination" means "any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to his performance in any test, work or other activity" thus written assessment work, field work etc. are covered.

Internal Examiners' comments

Internal examiners' comments, whether made on the script or in another form that allows them to be held and applied to the original script (e.g. in a coded table), will be covered by the 1998 Act. A data subject has the right to request that a copy or summary "in intelligible form" is provided within the stipulated timescale. This limit is normally 40 days, but in the case of examinations the Act specifically notes that a request may be made before results are announced. In this case there is a limit of five months from the request or 40 days from the announcement of the result, whichever is the earlier.

HE and FE institutions should ensure that internal examiners' comments on examination scripts, assessed work etc. are capable of being produced for a data subject in a meaningful form.

HE and FE institutions should ensure that internal examiners' comments on examination scripts, assessed work etc. are both intelligible and appropriate. Guidance as to correct form and procedure should be given to examiners where deemed appropriate.

HE and FE institutions should consider how the recording of internal examiners' comments could be made more appropriate for subject access (e.g. tear off comment sheets in examination script booklets).

External Examiner's comments

External examiner's 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), will be covered by the 1998 Act. A data subject has the right to request that a copy or summary "in intelligible form" is provided within the stipulated timescale. This limit is normally 40 days, but in the case of examinations the Act specifically notes that a request may be made before results are announced. In this case there is a limit of five months from the request or 40 days from the announcement of the result, whichever is the earlier

HE and FE institutions should ensure that external examiners' comments on examination scripts, assessed work etc.:

- are capable of being produced for a data subject in a meaningful form.
- are both intelligible and appropriate. Guidance as to correct form and procedure should be given to examiners where deemed appropriate

HE and FE institutions should consider how the recording of external examiners' comments could be made more appropriate for subject access.

Automatic processing

The 1998 Act provides data subjects with specific rights to be informed of the logic of any purely automated decision that significantly affects them. This may have some relevance to assessment and examinations, but major pass/fail or grade distinctions are rarely, if ever, made purely on the basis of automated decisions. HE and FE institutions will normally require that subject area examination boards review and validate the results of each candidate, taking into account such variables as personal circumstances, health issues etc. Candidates are also entitled to have an explanation of how automated processes such as degree classification software operate. In practice, HE and FE institutions usually already provide such explanation, as review of administrative procedures will normally be required in the event of a student appeal against classification etc.

HE and FE institutions should have:

- a formal statement that explains the logic behind any assessment that is based entirely on automated means, including single tests that form only a part of some larger assessment;
- a formal statement that explains the logic behind any classification or grading system that operates using automated means.

Examination Board Minutes and related documentation

Minutes of Examination Boards that contain discussion about data subjects will be subject to data subject access where candidates are named, or referred to by identifiers from which candidates may be identified (such as PINs), unless the data cannot be disclosed without additionally disclosing personal data about a third party.

Minutes of special circumstance committees that make decisions with regard to evidence supplied by candidates for reduced performance or non-performance in examinations, for the purposes of supplying recommendations for consideration by Examination Boards, will

be subject to data subject access where candidates are named, or referred to by identifiers from which candidates may be identified (such as PINs), unless the data cannot be disclosed without additionally disclosing personal data about a third party.

HE and FE institutions should provide:

- copies of those parts of minutes of examination boards that refer to the data subject who is making the subject access request, unless the data cannot be disclosed without additionally disclosing personal data about a third party;
- copies of those parts of minutes of special circumstance committees that refer to the data subject who is making the subject access request, unless the data cannot be disclosed without additionally disclosing personal data about a third party.

Disclosure of results

As personal data, examination results should not be disclosed to third parties without the data subject's consent. This does provide HE and FE institutions with some difficulties, as many institutions have traditionally publicly disclosed examination results in a variety of ways, including noticeboards, newspapers, graduation documentation etc. Indeed a number of institutions have an obligation in their statutes to publish results. The majority of students do not find these methods of disclosure harmful or distressing, indeed it is likely that there would be an outcry if they were abruptly ended. However, these methods of disclosure are usually of a local and limited nature. Posting examination and degree results on the Internet would clearly go beyond a local and limited distribution. It is difficult to argue that there is anything distressing or damaging about results being posted locally in public with names; on the other hand, individual cases have arisen where students have claimed that having their whereabouts made known put them at risk.

HE and FE institutions should provide:

- an explanation of where, and how, data subjects may expect to see their results posted;
- a mechanism through which data subjects can effectively exercise their right to object to their results being displayed in all or any particular fora.

HE and FE institutions should not:

- display results outside their local area (e.g. via the Internet) without obtaining the consent of the data subjects;
- in the absence of consent from the data subject, disclose results over the telephone, unless a suitable security system (e.g. passwords) is in place to ensure that the caller is in fact the relevant data subject;
- withhold results from candidates in financial arrears.

HE and FE institutions should consider:

- a mechanism for data subjects to indicate their consent to the institution displaying their results in particular fora;
- publishing results on publicly accessible noticeboards with PINs instead of names;
- providing results directly to each student face-to-face, via post, or via secure electronic means.

Use of Personal Data in Research

As under the 1984 Act, the 1998 Act provides certain exemptions for "research purposes" including statistical or historical purposes. s.33 of the 1998 Act exempts personal data used for research purposes from certain of the data protection rules. If the purpose of the research processing is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, it is exempt from:

- the second data protection principle, meaning that personal data can be processed for purposes other than for which they were originally obtained;
- the fifth data protection principle, meaning that personal data can be held indefinitely;
- the data subject's right of access to his personal data (s.7) where the data is processed for research purposes and the results do not identify data subjects.

s.33 does NOT give a blanket exemption from all the Data Protection Principles to data provided and/or used for research purposes. Researchers wishing to use personal data should be aware that most of the Data Protection Principles will still apply (notably the requirement to keep data secure) and there should be an assessment of the legality of processing on each occasion data are provided for research purposes. Periodic assessment of the nature of data protection procedures and practices in research areas should be carried out.

The *Data Protection (Processing of Sensitive Personal Data) Order 2000* para.9 provides that processing in the course of maintaining archives for research purposes is permissible where the sensitive personal data are not used to take decisions about any person without their consent and no substantial damage or distress is caused to any person by the keeping of those data.

HE and FE institutions should ensure that:

- employees and students are aware that, while some exemptions are granted for the use of personal data for research purposes, the majority of the Data Protection Principles must still be conformed to – there is no blanket exemption.
- in all circumstances where personal data is to be used for research purposes that there has been an adequate review, in advance of processing, to ensure that the requirements of the 1998 Act can be adhered to.
- data protection procedures and practices in research areas are monitored periodically to ensure adequate compliance.
- 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
- particular care is taken when the processing involves sensitive personal data.

HE and FE institutions are advised always to provide as clear guidance as possible 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.

Confidential References

References given by HE and FE institutions

Confidential references given by HE and FE institutions, including, references written by written by employees in their formal capacity, or as part of a standard procedure, (for example, as Head of Department, as part of a promotions exercise) are exempted from subject access requests where those references relate to:

- education, training or employment of the data subject
- appointment of the data subject to any office
- provision by the data subject of any service.

HE and FE institutions have the absolute discretion to refuse to release confidential references written on their behalf if requested to do so in, or as part of, a subject access request.

References received by HE and FE institutions

Confidential references received by HE and FE institutions are not exempt from the right of access, but consideration must be given to the data privacy rights of the referee. Information contained in, or about, a confidential reference need not be provided in response to a subject access request if the release of this information would identify an individual referee unless:

- the identity of the referee can be protected by anonymising the information;
- this referee has given his/her consent, or;
- it is reasonable in all the circumstances to release the information without consent.

In cases where a confidential reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights.

HE and FE institutions, when faced with the question of subject access to a reference received in confidence from a referee, must consider what steps have been taken to try and obtain consent, whether the referee has expressly refused to give their permission for the information to be made available, and whether the disclosure might result in harm to the referee.

HE and FE institutions may not refuse to disclose references received in confidence from third parties without providing reasons.

HE and FE institutions should consider:

- routinely informing third parties who will be providing references of their policy with regard to disclosure of confidential references;
- requesting that third parties who will be providing references state unequivocally whether or not they object to the reference being released to the data subject in the event of a subject access request;
- providing guidance to their staff as to acceptable form and content in references;
- providing advice as to appropriate avenues of action in circumstances where staff do not feel that an applicant is suited to the job/course. .

References internal to HE and FE institutions

There may be circumstances where a confidential reference is written on behalf of a data subject by an individual in one department of an HE or FE institution, to be used by an individual in the same institution or even the same department. There is no obvious justification for differentiating between confidential references received from external third parties and confidential references received from within the institution as regards any consideration of data subject access.

HE and FE institutions, when faced with the question of subject access to a reference sent and received internally, should apply the same criteria to the reference upon receipt of a subject access request, as they would to a reference received from an external third party.

Transfers of Personal Data to non-EEA Countries

The Data Protection Act 1998 contains specific provisions with regard to the transfer of personal data to countries outside the EEA (the EU Member States, plus Norway, Iceland and Liechtenstein). The eighth data protection principle states "'Personal data shall not be transferred to a country or territory outside the 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." This is qualified by a number of conditions set out in Schedule 4 DPA 1998, for example, personal data may be transferred to a country without an adequate level of protection where the data subject has given his consent to the transfer.

There will be two elements involved when determining the adequacy of protection of data privacy in a non-EEA country to which personal data are to be transferred.

- the substantive rules that apply to protection of the data;
- the methods of enforcement by which compliance with those substantive rules is attained.

The first of the elements can be achieved by ensuring that the substantive rules that apply to the transferee have the same effect as those contained in the Act. There are a number of ways that this could be achieved: national legislation in the jurisdiction to which the data are transferred; codes of conduct at an industry or sectoral level; or specific contractual provisions between the UK-based transferor and the transferee; or elements of all three. However, the second element poses a thornier problem, it is difficult to see, for instance, how data subjects might be provided with similar private legal rights of action against non-EEA data transferees to those that they have available against EEA-based transferees under the Act.

The ODPC has produced a preliminary guidance note entitled "The Eighth Data Protection Principle and Transborder Dataflows" which provides a detailed legal analysis and suggests a "good practice approach" to assessing adequacy, including consideration of the issue of contractual solutions.

HE and FE institutions should:

- have particular regard to the recommendations in the ODPC preliminary guidance note "The Eighth Data Protection Principle and Transborder Dataflows" when determining whether or not a country has adequate protections for personal data in relation to the proposed transfer;
- the proper procedure to adopt for transfer of personal data to non-EEA countries.
- consider whether or not and, if so, the extent to which, a decision to treat the third country as adequate in relation to the proposed transfer will prejudice the fundamental rights and freedoms of the data subject(s), and in particular their right to privacy with respect to the processing of personal data"
- be able to justify any decision they make about adequacy should it prove necessary for the ODPC to enquire as to the basis for any transfer to a third country

HE and FE institutions should:

- consider whether specific transfers of personal data to a non-EEA country may be necessary:
- for the performance of a contract between the data subject and the data controller, or
- for the taking of steps at the request of the data subject with a view to their entering into a contract with the data controller, or
- for the conclusion of a contract between the data controller and a person other than the data subject which was entered into at the request of the data subject, or is in the interests of the data subject, or for the performance of such a contract.

  Such transfers are exempted from the prohibition on transfer. Examples in the HE and FE sector would include: requests by HE and FE institutions to non-EEA governments, agencies, and organisations for information necessary to determine academic eligibility for attending a course of study in the UK; transfers of personal data to non-EEA governments, agencies, and organisations sponsoring students to attend a course of study in the UK, where such sponsorship is dependent upon attendance and/or performance criteria; transfers of personal information (e.g. examination marks), relating to, and required by, data subjects engaged in distance learning courses.
- be able to justify any decision they make about exempted transfers should it prove necessary for the ODPC to enquire as to the basis for any transfer to a third country

HE and FE institutions should in most other circumstances, obtain the specific and informed consent of the data subject before transferring personal data to a non-EEA country, that is

- the data subject should be made aware of the risks that the institution may have assessed as being involved in the transfer; and
- the data subject should have given clear consent to the transfer.

  The institution should be able to produce clear evidence of the data subject's consent in any particular case and be able to prove that the data subject was informed as required. Consent in writing is thus recommended, unless the institution has suitable technological means to ensure that authenticated consent can be collected on-line. An example in the HE and FE sector would be the transfer of staff personal data to a non-EEA country to be used in the management of a distance learning course. Where a data subject requests a reference be written and sent to a non-EEA country, the request itself will indicate their consent to the personal data transfer.

HE and FE institutions should not:

- in the absence of a sponsorship arrangement, 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 purposes of determining liability to attend National Service, without the specific and informed consent of the data subjects concerned.

The Internet and World Wide Web

General Institutional Webpages

Most HE and FE institutions now have an Internet presence, normally in the form of a website containing a range of information about the institution and accessible world-wide, and an intranet, again usually web based, but only accessible to members of the particular institution. Within the set of webpages that make up both institutional Internet and intranet websites there will be webpages that contain personal data such as staff names, pictures, contact details etc.

Such data, when released on the Worldwide Web, by definition goes beyond the E.E.A., including to countries that do not have data privacy regimes considered adequate by the EU Commission, and therefore contravenes the Eighth DP Principle unless (for example) one has the consent of the data subject. Even without this technicality, it is a very open form of publication, and data subjects should be able to exert their normal rights (as in DP Principle 6). Where HE and FE institutions use personal data in this way consideration needs to be given to the reasons for the display of the data.

Staff personal data which is required to be supplied for the purposes of the normal organisational functioning and management of the institution and, in particular, information which is already supplied in publicly available hardcopy publications such as Calendars and prospectuses should not require the consent of data subjects to be placed on an institutional Internet or intranet website. However, data subjects whose personal data is used in this way should be informed of this use and must still retain the right to object to the use of their data where it would cause them significant damage or distress.

All other non-essential uses of personal data on an institutional Internet or intranet website, including the use of photographs of data subjects (background shots, panoramas etc.) where the data subject is clearly identifiable will normally require the institution to make reasonable efforts to ensure that it has obtained the consent of the relevant data subjects. If consent cannot be obtained, for example because the data subject is untraceable, the institution should consider whether the use of the personal data might reasonably be considered likely to cause the data subject damage or distress. Where consent is refused, the personal data in question should not be used.

HE and FE institutions may use non-sensitive staff personal data on institutional Internet and intranet webpages without consent where:

- its display facilitates the normal organisational functioning and management of the institution. This may be indicated by its inclusion in existing publicly available hardcopy publications.
- staff are informed that certain personal data will be displayed on institutional webpages, and have the right to object to the use of their data where it would cause them significant damage or distress. Retaining the right to object does not mean automatically being able to have data removed, rather that the data subject is in a position to make their objections known - the institution can then make a determination on whether the damage or distress alleged is a suitable ground for removal.

HE and FE institutions should make all reasonable efforts to obtain the consent of all data subjects, staff and student, where non-sensitive personal data (including photographs) is to be used on institutional Internet and intranet webpages and in other publications, where such use is not for the purposes of the normal organisational functioning and management of the institution (e.g. publicity photographs etc.).

HE and FE institutions should not use sensitive staff or student personal data on institutional Internet or intranet webpages without explicit consent unless those webpages are only accessible to the data subject.

Institutional Staff and Student Directories

Staff and student on-line telephone and e-mail directories (including the X500 database), being essential to the organisational functioning and management of HE and FE institutions, should not require the consent of the data subjects, if restricted to use on an institutional intranet. However, data subjects whose personal data is used in this way should still retain the right to object to the use of their data where it would cause them significant damage or distress.

Where staff on-line telephone and e-mail directories are made available on the Internet, for the purposes of the normal organisational functioning and management of the institution, this should not require the consent of data subjects. However, data subjects whose personal data is used in this way should be informed of this use and should retain the right to object to the use of their data where it would cause them significant damage or distress.

Where student on-line e-mail directories are made available outside the institution, this will not be for the purposes of the normal organisational functioning and management of the institution and thus consent should be obtained from data subjects and they should be able to opt out of having their details displayed.

While consent, and even explicit consent might be capable of being inferred from actions e.g. clicking on an "OK" button on the institution's website in response to the question "Do you consent to your e-mail address being displayed on the University's Internet webpages?" it is probably easier in the long term to collect consent in writing at the time of initial registration/employment. Opt out should be capable of being exercised at any time.

HE and FE institutions may use institutional staff and student on-line telephone and e-mail directories on restricted access intranets where:

- these facilitate the normal organisational functioning and management of the institution.
- staff and students are informed that certain personal data will be included in such directories, and have the right to object to the use of their data where it would cause them significant damage or distress

HE and FE institutions may use staff on-line telephone and e-mail directories on Internet web sites where:

- these facilitate the normal organisational functioning and management of the institution.
- staff are informed that certain personal data will be included in such directories, and have the right to object to the use of their data where it would cause them significant damage or distress

HE and FE institutions should obtain consent from student data subjects before including their personal data in on-line e-mail directories available on an institution's Internet website, and student data subjects should be able to opt out of having their details displayed.

Web pages used to collect personal data

Many HE and FE institutions use web pages to collect personal data, such as names and addresses of individuals who request documentation e.g. prospectuses. It is important that the rationale for data collected is clear, and that no personal data other than that which is required for the particular transaction is collected. Use of web browser "cookies" to track users of institutional websites should be carried out for specified reasons, and not just because the software permits it.

HE and FE institutions should ensure that at the point of collection (i.e. on the relevant web page) the following information is provided to the data subject:

- the purpose for which the data is collected
- the recipients or classes of recipients to whom the data may be disclosed
- an indication of the period for which the data will be kept (e.g. "while we process your application", "for the duration of your studies" etc. rather than a specific time period.)
- and any other information that may be required to ensure that the processing is 'fair'

HE and FE institutions should provide the ability to opt out of any parts of the collection of, or use of, the data that are not directly relevant to the intended transaction (e.g. where an individual provides their name and address to an institution in order to obtain a prospectus, if the institution runs a follow up scheme designed to discover why candidates did not come to that institution, the individual should be notified of that scheme and be able to opt out of it)

HE and FE institutions should ensure that subsequent use of the data conforms to the information provided to the data subject, and before any further subsequent use that was not disclosed at the time of collection further consent must be obtained from the data subject.

Personal employee and student webpages on institutional machines

In many institutions, employees and students have been permitted to create personal web pages on institutional servers, or even to run their own web servers. This policy approach has been justified on the grounds that use of such facilities serves an educational purpose and the services were either unavailable elsewhere, or were too costly for the average user. The rise of free Internet Service Providers (ISPs) such as Freeserve and free email suppliers such as Hotmail has provided institutional users with other options.

FE and HE institutions should ensure that all individuals running personal web servers on institutional equipment or with personal web pages hosted by the institution are aware of their obligations under the 1998 Act.

HE and FE institutions should consider:

- whether employees and students should be permitted to run personal webservers or to have personal webpages on institutional machines where such webservers and webpages are used for purposes unconnected with their employment or studies
- the terms and conditions under which such personal webservers or personal webpages should be permitted, if allowed.

Internet and Intranet Monitoring

In the business environment, it is becoming the norm for companies to routinely monitor all data held on their equipment and to inspect all e-mail and other electronic data entering, leaving, or within, their networks. FE and HE institutions require the ability to inspect all data held on their computer equipment, and to inspect all e-mail and other electronic data entering, leaving, or within, the University network to ensure conformity with:

- Institutional regulations
- Contractual agreements with third parties
- UK law

FE and HE institutions are obliged by virtue of the agreement entered into with UKERNA to ensure as far as possible that their users do not use the SuperJANET system to transmit or transfer certain types of electronic data. They are obliged by law to report to the police the discovery of certain types of electronic data, if that data is found on their equipment, or transmitted across their networks.

Many types of routine computer service tasks will involve members of FE and HE institutions' staff (such as network administrators) having access to various levels of staff and student held data. Examples include:

- network administrators' using of logfiles for administrative purposes.
- e-mail postmasters receiving mail failure notifications will often be sent the text of the failed message by the e-mail server which has rejected or redirected it.
- staff making archive copies from fileservers will, as part of the archiving process, often be able to read the names of files held in staff and student accounts.
- staff sorting output from printers prior to its dissemination to users will be able to view the content of that output.

It is inevitable that under these routine circumstances, members of staff will, on occasion, and in the course of their legitimate organisational functions, be required to access, process and possibly disclose personal data held on FE and HE institutions' computers systems. Internal guidelines should be provided to ensure both those running institutional computer systems and those using them are aware of the circumstances under which their personal data may be accessed, processed and disclosed and the safeguards against misuse of that personal data.

HE and FE institutions may permit authorised staff to access, process and disclose personal data held on institutional computer systems, where this is required in the course of their legitimate organisational functions, and where the institutions are required to comply with legal and contractual obligations

HE and FE institutions should ensure that:

- authorised staff are adequately informed of the circumstances in which they may legitimately access, process and disclose personal data held on institutional computer systems
- institutional computer system users are adequately informed of the circumstances in which authorised staff may legitimately access, process and disclose personal data held on institutional computer systems

HE and FE institutions should provide:

- a mechanism for data subjects to object to the accessing, processing and disclosure of their personal data held on institutional computer systems where it would cause them significant damage or distress
- a mechanism for data subjects to ensure that where personal data held on institutional computer systems is accessed, processed or disclosed for legitimate organisational functions, or where the institutions are required to comply with legal and contractual obligations, it is not misused for other purposes

Collection and Processing of Personal Data relating to Disability

A key area where HE and FE institutions will need to collect and process sensitive data is that of service provision for disabled employees and students, as there is an obvious correlation between the disclosure of disability status and the ability of institutions to ensure that as full a range of services as possible can be supplied. Institutions will often collect student disability information at the admission stage (for example, through UCAS, and through the reference letters, interviews etc.), and employee disability information at interview stage but collection of disability data may also occur throughout the period of study or employment. The use of "blanket" consent forms is inappropriate for many forms of data collections, but particularly so for collection of sensitive personal data, including disability data.

Where an individual refuses to consent to disclosure of a disability in a reference, the referee must decide if they can write a reference under those circumstances, reflecting their duty of care to both the individual and the person or organisation requesting the reference. If a referee feels that they cannot meet their duty of care to either party under those circumstances, they should inform the individual that they will be unable to write an complete reference without referring to the disability, and that this would not be in the best interests of either the individual, the person or organisation requesting the reference, or the institution providing the reference. If consent is still unforthcoming, no reference should be written.

HE and FE institutions should provide:

- mechanisms to ensure that where disability data is provided for a stated purpose, such as to ensure adequate service provision, it is not misused for other purposes, such as to make a decision about whether or not to admit a student to a course of study
- safeguards to protect disabled employees and students against discrimination, harassment, and victimisation that may arise from disclosure of their disability status.
- clear and readily accessible remedies for disabled employees and students in cases where they suffer distress or damage due to misuse of the information about their disability status.
- a system whereby when there is a need to disclose disability data to external organisations, prior consent of the data subject can be obtained for each disclosure and the nature of the information to be disclosed, the intended recipient, and the purpose of disclosure can be provided to the data subject.
- procedures that both protect an individual's privacy and permit necessary disclosure for the provision of effective support for disabled employees and students or to ensure health and safety.

HE and FE institutions should provide adequate information to all applicants, students and staff regarding institutional policies relating to the confidentiality and disclosure of personal information on disabilities, including information that is gathered for monitoring purposes. This should outline the:

- parties to whom the institution is obliged to disclose disability information;
- parties who will be automatically told of the disability unless the student objects;
- parties who will only be told if specific consent is obtained.

Counselling Services

Most HE and FE institutions provide Counselling Services for employees and students. Such Counselling Services will, in the course of their ordinary operations, be legitimately collecting and processing personal data, including sensitive personal data (See *The Data Protection (Processing of Sensitive Personal Data) Order 2000*, s.4).

HE and FE Employee and Student Counselling Services should provide clients with:

- guidance to the service's personal data policies on data collection and retention
- guidance on access to counsellors' notes and other records that refer to them
- a timescale for destruction of the client's personal data.

HE and FE Employee and Student Counselling Services should:

- make acceptance by the client, of the service's record-keeping practices, part of the contract with the service.
- take all reasonable steps to ensure that counsellors, administrative staff and trainees respect the need for confidentiality regarding any information obtained.
- permit counsellors to discuss a client's records with that client, whilst ensuring that, in such discussions, references to third parties are withheld.
- ensure all records are kept securely and remain confidential within the service.
- provide for the secure disposal of personal data that is no longer required

HE and FE Employee and Student Counselling Services should ensure total confidentiality of client personal data, subject only to the following exceptions:

- where the counsellor has the express consent of the client to disclose the data;
- where the counsellor believes that the client is a serious danger to themselves, that their GP should be informed of that fact so that appropriate steps can be taken to ensure their safety, and that to inform the client of the disclosure would increase the level of risk;
- where the counsellor believes that serious harm may befall a third party if the data were not disclosed;
- where the counsellor would be liable to civil or criminal court procedure if the data were not disclosed.

HE and FE Employee and Student Counselling Services may keep "risk registers" of various types, including:

- names of individuals who a counsellor believes may be at especial risk of self-harm, and who will require careful management if seen on a drop-in basis or if their counsellor has to cancel an appointment;
- names of individuals who may be violent, so that counsellors can check before they arrange one-to-one meetings.

Access by counsellors to such "risk registers" should be available only on a "need to know" basis. Inclusion on a "risk register" may not be disclosable to a data subject under subject

access on the grounds that the health & safety of the data subject, or counsellors, may be at stake (s31(2)(e)).

HE and FE Employee and Student Counselling Services should ensure that where counsellors discuss casework with supervisors:

- such discussion should be in general rather than specific terms, so that personal circumstances may be revealed, but not the identity of the client; or
- the client should be informed in advance that the that counsellor may discuss their case with a supervisor should they feel it necessary.

HE and FE Employee and Student Counselling Services should ensure counselling members of staff are bound by a Code of Ethics and Practice (e.g. the British Association for Counselling (BAC) Code of Ethics, or the British Psychological Society Code of Conduct).

Careers Services

Most HE and FE institutions provide Careers Services for students. Such Careers Services will, in the course of their ordinary operations, be legitimately collecting and processing personal data, including sensitive personal data (See *The Data Protection (Processing of Sensitive Personal Data) Order 2000*, s.4).

HE and FE institutions' Careers Services should provide students with:

- guidance to the service's personal data policies on data collection and retention
- guidance on access to advisors' notes and other records that refer to them
- a timescale for destruction of students' personal data held for careers purposes.

HE and FE institutions' Careers Services should

- make acceptance by students of the service's record-keeping practices part of the contract with the service.
- take all reasonable steps to ensure that advisors, administrative staff and trainees respect the need for confidentiality regarding any information obtained.
- permit an advisor to discuss a student's records with that student, whilst ensuring that, in such discussions, references to third parties are withheld.
- ensure total confidentiality of student personal data, subject only to the following exception; where the advisor has the express consent of the student to disclose the data (e.g. to potential employers).
- ensure all records are kept securely and remain confidential within the service.
- provide for the secure disposal of personal data that is no longer required.

HE and FE institutions' are legally obliged by the Higher Education Statistics Agency to collect first destination data for graduating students. Careers Services are usually tasked with collection of this data. Careers Services should ensure that personal data collected for HESA purposes is only supplied in unanonymised form to HESA. All other uses of the data internal or external to an institution should be in the form of anonymised data unless the consent of the data subject has been obtained in advance.

Other Information

Next of Kin/Emergency Contact Information

Access to a data subject's emergency contact details may play a vital part in ensuring the data subject's health and safety. However, the potential benefits of any disclosure of personal data must still be weighed against the potential hazards, particularly where the data controller decides that it is not necessary for him to notify the data subject. In view of the potential importance of the emergency contact details, and the limited potential for damage or distress to the data subject, collection of personal data without informing the data subject or obtaining their consent will be viewed as acceptable practice. In addition, staff and students at HE and FE institutions should be given the opportunity and ability to amend emergency contact details at any time, and in any event should be prompted to ensure their accuracy at yearly intervals.

HE and FE institutions will act within acceptable practice if they collect 'emergency contact details' from staff and students without the consent of the individual or individuals to be contacted, where:

- staff and students are advised via the collection form that emergency contact data will only be used only for emergency purposes
- the emergency contact data will only be disclosed in emergency situations in the immediate health or safety interests of the staff member or student;
- staff and students are advised via the collection form that they should notify the individual or individuals to be contacted of the disclosure to the institution of the individual's or individuals' details;
- obtaining the consent of the individual or individuals to be contacted would involve disproportionate effort.

Applications for Access Funding and other discretionary funding

Students may be allocated funds from money given to HE and FE institutions by the DFEE for the provision of Access Funds. Students will normally be invited to apply for help and complete an application form. Decisions on whether to allocate funds to individual students are often made on the contents of their application form and/or on the basis of confidential references. Students are entitled to have access to any personal data held by the institution with regard to an Access Fund application, unless the data cannot be disclosed without additionally disclosing personal data about a third party. These criteria should also apply to any other application for discretionary funding.

HE and FE institutions should ensure that internal assessors' comments on applications for Access Funds or other discretionary funding are capable of being produced for a data subject in a meaningful form.

HE and FE institutions should ensure that internal assessors' comments on applications for Access Funds or other discretionary fundingare both intelligible and appropriate. Guidance as to correct form and procedure should be given to assessors where deemed appropriate.

Alumni Records

While UK HE institutions do not yet pursue their alumni as assiduously as North American institutions, alumni are clearly a potentially valuable source of funding. An important first step is to be able to locate and correspond with them. Alumni offices often adopt practices resembling (or indeed identical) those of the direct mail industry. Where this is the case, an alumni database will not only have to conform with the data protection principles, but will also have to take account of the fact that data subjects can request that their personal data are not processed for direct marketing purposes.

HE and FE institutions should ensure that:

- students are informed at the time of the collection of their personal data for an alumni database that the institution will wish to maintain contact with them after they finish their course of study, and the reasons why.
- students and alumni are able to opt out of the collection and processing of their personal data for such purposes.
- students and alumni are able 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.
- students and alumni are provided with mechanisms whereby they can obtain the rectification, blocking, erasure, and destruction of their personal data, if necessary.
- HE and FE institutions should consider implementing mechanisms permitting students and alumni to access and correct their data remotely (e.g. passworded Internet access to their alumni database record)

CCTV and similar surveillance equipment

HE and FE institutions are increasingly using Closed Circuit Television and similar surveillance systems (hereafter referred to as CCTV) across their sites to ensure site security and the safety of staff, students and visitors. Users of CCTV will need to comply with the provisions of the 1998 Act as these systems invariably require the processing of personal data.. The Data Protection Commissioner has issued a code of practice in accordance with her powers under s51 (3) (b) of the 1998 Act for users of CCTV and similar surveillance equipment monitoring spaces to which the public have access. Compliance with this Code of Practice, notably those standards that are directly based on the Data Protection Principles and Act, will aid users of CCTV systems in meeting their legal obligations. Compliance with the Code of Practice will also factor into any determination by the Data Protection Commissioner as to whether institutions have made proper use of CCTV.

HE and FE institutions should:

- adopt a form of the "Code of Practice for users of CCTV and similar surveillance equipment monitoring spaces to which the public have access," with such revisions as are required for their individual circumstances;
- audit their compliance with the Code of Practice requirements on a regular basis.

Retention of Records containing Personal Data

This list is not exhaustive, but provides guidance as to best practice. For further detailed advice on document retention see the JISC publication "Study of the Records Lifecycle."

Type of Record	Suggested Retention Period	Reason for Length of Period
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation.
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence At least 10 years for personal and academic references. Certain personal data may be held in perpetuity.	Limitation period for negligence. Permits institution to provide references for a reasonable length of time. While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.