Cambridge University Data Protection Act 1998 Working Party

Report to Council, July 2000

(The recommendations contained in this report are repeated, collected together for reference, in section 19.)

1. Background

The Data Protection Act 1998 (**the Act**) came into force in March 2000, replacing the Data Protection Act 1984.

Preliminary advice about the Act was circulated within the University in a memorandum to all Departments by the University Data Protection Officer (UDPO) (Document DB-L/492/2 of 10 August 1998).

In response to the passing of the Act, the University Council (Council minute 129(b) 25 January 1999) established the Data Protection Working Party (DPWP) to 'consider the issues and to bring forward policy and procedural proposals to the central bodies'. The members of the DPWP are listed in Annex 1. It met 5 times from 12 Jan 2000 to 7 June 2000 inclusive. This document is the report of the Working party to the University about the implications of the Act for the University. Whilst the Colleges are autonomous bodies and will have separate notifications under the Act, this report discusses issues affecting both the University and Colleges, and therefore may be of interest to Colleges.

The Act is complex, and in many important respects its interpretation is not yet certain. The **Data Protection Commissioner** (an office created by the Act to replace the office of "Data Protection Registrar") and her staff have issued guidance, but this does not necessarily have the force of law. There remain many grey areas, and the Office of the Data Protection Commissioner (henceforth ODPC) is itself awaiting further clarification from the Government on a number of issues (including, for example, the sections of the Act which deal with the transfer of data outside of the European Union). Some matters of interpretation may remain uncertain until they have been determined by test cases in the courts. Different organisations, taking more or less cautious approaches, therefore give different advice on what the Act implies.

Codes of practice are being prepared on behalf of Joint Information Systems Committee (JISC), for approval by the Data Protection Commissioner, by Andrew Charlesworth, Senior Lecturer in IT law at the University of Hull. In early June, drafts of these codes of practice were received; they have been taken into account and are included as annexes to this document.

If the proposed Freedom of Information Act is passed, it will modify the Data Protection Act. The implications of this are considered later in this report.

In many areas, the Working Party recommends in this report that the University must decide a policy. Such recommendations are made not only because it is good practice to operate within an agreed and clearly defined policy framework, but because

- in response to Data Subject access requests (explained later) the University must respond within a time limit (generally 40 days) and a significant fraction of this time will be required simply to locate, screen and copy the relevant data. It is therefore important that policy issues are clear in advance.

- the Working Party was advised that in the event of disputes, and for example appeals to the Data Protection Commissioner, the existence of an agreed policy is in itself valuable to the University in defending its decisions.

2. Summary of the provisions of the Act

The Act is much wider ranging than the Data Protection Act 1984. Annex 2 describes its provisions and explains the differences from the 1984 Act. In summary, the new Act:

- governs **Personal Data**, with additional restrictions in relation to **Sensitive** Personal Data. The living individual to whom such data relates is called the **Data Subject**.
- regulates all **processing** of Personal Data, defining 'processing' so widely that "it is difficult to imagine any action involving data which does not amount to processing" [2]; **processing** includes obtaining and holding data.
- covers **Structured Manual Records** as well as electronically held records. Manual Records include, for example, paper or microfiche records. The term 'Structured' refers to the definition in the Act of a **relevant filing system** as "any set of information relating to individuals … structured … in such a way that specific information relating to a particular individual is readily accessible".
- defines conditions under which Data Processing is permitted, requiring that it should be fair (as defined by a **fair processing** code) and lawful, and that it must not take place unless at least one specified condition is met. Further conditions must be met prior to the processing of Sensitive Personal Data.
- is no longer restricted to processing 'by reference to the data subject' - for example, it would now cover listing the ages of all staff of a certain type – even if names are not part of the extracted data.
- extends the rights of **Data Subjects** to be told the purposes for which information is being Processed, the likely recipients of the data, and the sources of the data. Gives the Data Subject certain rights to be provided with a copy of the data, to amend errors, and to prevent various types of Processing.
- imposes a new **notification** process, which replaces the old registration process, but has wider ranging consequences for the University, because 'blanket' declarations of purpose are no longer acceptable.
- imposes an obligation on the University to take "appropriate technical and organisational measures to prevent the unauthorised or unlawful Processing of Personal Data …", in other words to have appropriate **security systems and procedures** for (both electronic and manual) data.
- imposes significant restrictions on the **transfer of data** outside the European Economic Area. These affect, amongst other things, the placing of Personal Data onto the World Wide Web
- imposes new requirements when data is transferred into or out of the University, for example to third parties for processing.

2.1 Transitional Provisions

However, substantial relief is offered by **Transitional Provisions** in the Act. These are described in Annex 4. In summary:

- Data is **eligible** for the transitional exemptions if the processing to which the data is to be subjected was already underway on 23 October 1998 (or if the data is to be used for closely related purposes). Note that the data itself is permitted to have been obtained after that date.
- Eligible **automated** (i.e. electronically held) data is exempt from most of the new provisions of the Act (that is, "new" compared to the 1984 Act) until 23 October 2001.
- Eligible **manual** data is exempt from most of the provisions of the Act (including Data Subject Access rights) until 23 October 2001.

For data subject to processing which was already underway on 23 October 1998, where the **data itself was already held** on 23 October 1998, there are some further limited but significant transitional

exemptions. Such data do not have to meet the new standards (such as accuracy and relevance) required of data collected after that date, until 23 October 2007. However, there will be rights of subject access to this data from 24 October 2001.

2.2 Conditions for processing Personal Data

As well as the requirement that data be processed 'fairly' (for example by adhering to the 'Fair Processing Code'), personal data may only be processed provided at least one of the conditions listed in Schedule 2 of the Act applies. The following are the two conditions most likely to be relevant:

- The processing is necessary for the purposes of legitimate interests pursued by the University; or
- The data subject has given their consent to the processing.

In the memo of August 1998, it was suggested that Departments should ensure that consent is gained from the Data Subject for any of their data that the department holds. The Working Party believes that this is not the best policy, as explained in section 3.

2.3 Conditions for processing Sensitive Personal Data

'Sensitive Personal Data' are defined as personal data consisting of information as to the Data Subject's: racial or ethnic origin, political opinions, religious or similar beliefs, membership of trade unions, physical or mental health conditions, sexual life, commission or alleged commission of any offence, or proceedings for any offence committed or alleged to have been committed by the subject.

The processing of sensitive personal data requires not only one of the Schedule 2 conditions to apply, but also one of the further conditions listed in Schedule 3 of the Act. For many purposes in the University, the only relevant Schedule 3 condition is likely to be that

- the Subject has given their 'explicit consent'.

Two other relevant conditions from Schedule 3 are that the processing is necessary

- for medical purposes, including medical research – provided it is carried out by a health professional or a person who owes a duty of confidentiality equivalent to that which would be owed by health professional – and
- for monitoring equality of opportunity etc. – under "appropriate safeguards for the rights and freedoms of the data subjects". The specific rules are given in the "Data Protection (Processing of Sensitive Personal Data) Order 2000".

2.4 Exemptions from the normal conditions

The Act permits processing for various "special purposes". These include

Research purposes (which includes statistical or historical purposes, including archival) – subject to specific rules and restrictions. These are described in Annex 5.

Journalism, Artistic, or Literary purposes, subject to various rules. These include a requirement that the data processing is with a view to publications, and that the Data Controller (the University) believes that such publication would be in the public interest.

Specific further exemptions, such as those related to Confidential References written by the University, and to Examination Scripts, are discussed in relevant sections later.

2.5 Information which must be supplied to the Data Subject

When data are collected, the data subject must be told the purpose(s) for which their data will be processed. This is part of the 'Fair Processing Code' in the Act. The Data Subject should also be told the identity of the Data Controller (the University) and the name of its representative (the University Data Protection Officer).

This information has to be given at the time of collecting the data or as soon as possible afterwards.

Note that data collected for given purpose(s) can only legitimately be processed for those purpose(s) – not for others of which the Data Subject has not been informed. We therefore recommend that the 'purposes' for which data is to be processed should be defined as broadly as is reasonable to the Data Subject. Although the ODPC has not yet published the proposed standard template for Universities, it is our belief that the definitions of 'purposes' in that template will be desirably broad.

Data Subjects have a right to be supplied on request with a description of their personal data that is held by the University. The regulations governing the procedure are in the Act, and are already in effect in the University.

All University Employees and Students should be made aware (see section 15.6) that any requests for access to personal data held by the University should be referred to the University Data Protection Officer, who will administer this process.

2.6 Other rights of the Data Subject

The Act gives the Data Subject the right to apply to the Data Controller (the University) to require the Processing to cease, on the grounds that it causes unwarranted substantial damage or distress to him or another. The University must respond either by agreeing to cease the processing, or giving reasons why it does not intend to cease the processing. In cases of dispute, the matter will be determined by the Courts.

Although the above right is subject to certain limitations (for example, it does not apply if the processing is necessary for the performance of a contract to which the Data Subject is a party, or for compliance with legal obligations of the University), the right does apply in the important case in which the stated reason for processing is that it is "necessary for the purposes of legitimate interests of the University".

There is a specific right of Data Subjects to require processing for purposes of Direct Marketing to cease.

A Data Subject may also apply to a Court, on the grounds that the Personal data are inaccurate, to require the University to "rectify, block, erase or destroy" that Data (and any other Data which in consequence is inaccurate).

3. Policy on conditions in which data subject consent should be sought

In the memo of August 1998, it was suggested that Departments should ensure that consent is gained from the Data Subject for any of their data that the department holds. However, where processing is "necessary for the purposes of legitimate interests pursued by the University" then the University is entitled to process non-Sensitive data without consent. Seeking consent in such a case, and then continuing with the data processing if consent is not given or is withdrawn, might provoke misunderstanding and time consuming complaints.

The DPWP therefore concluded that consent should only be sought in cases where the processing is not necessary for the purposes of legitimate interests pursued by the University. In such cases, provision must be made for ceasing the processing if consent is not given, or is subsequently withdrawn.

However, the right of the Data Subject to object to the use of their data where it would cause them significant damage or distress (section 2.6 above) remains. Thus for example in the draft Codes of Practice drawn up for JISC (e.g. Annex 10), the following text appears: "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."

Therefore it remains necessary in principle for the University to handle individual exclusions from Data Processing which is otherwise regarded as "necessary for the purposes of legitimate interests pursued by the University".

4. Manual files – general principles

The Working Party received a carefully argued paper which considered under what circumstances Manual Files (such as paper files) form part of a "relevant filing system". The relevant question is whether the set of data is "structured in such a way that specific information relating to a particular individual is readily accessible".

The Working Party accepted that there could be paper files which fell outside the definition of a "relevant filing system". For example, minutes of committees in which a particular individual's name happened to appear might well do so. However, it was concluded that where the intention behind a filing system was that it should be possible to find information about a specific person, then that filing system was extremely likely to fall within the definition of a "relevant filing system".

The Working Party believes that members of the University should be advised to assume that any filing system intended to contain accessible information about living individuals is a "relevant filing system" within the scope of the Act. Cases in which there is real uncertainty should be discussed with the University Data Protection Officer.

The Working Party also concurs with the advice given by the University of Sussex to its employees that "Restructuring of filing systems to get around the Data Protection legislation is strongly discouraged".

4.1 The Impact of the Freedom of Information Bill

The Freedom of Information (FoI) Bill, if its current draft provisions become an Act, will modify the DPA98. Under this Bill, the University will be a "public authority" because (within schedule 1 of the FoI Bill, para 57) we are "A university receiving financial support under section 65 of the Further and Higher Education Act 1992". In para 60 of the FoI Bill, Colleges also appear to be defined as "public authorities".

The FoI Bill [clause 67] will amend the DPA98 by adding to the definition of data a new category, (e): any data which is "recorded information held by a public authority and does not fall within any of the [existing categories of the DPA]." (this will bring within the DPA98 manual files which are not a "relevant filing system".)

Clause 69 will then cause this category (e) data to be exempt from most of the provisions of the DPA, except that it must be accurate, and the Data Subject has access rights (to be informed about, and have access to, the data). However, it will further completely exempt personal data which "relate to

appointments or removals, pay, discipline, superannuation or other personnel matters in relation to … service in any office or employment under … any public authority". This appears to completely exempt unstructured University and College files concerning employment matters, but not, of course, unstructured tutorial and similar files which relate to students.

Clause 68 will amend the DPA by defining "unstructured personal data" as category (e) data "other than information which is recorded as part (or with the intention that it should form part) of any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals". (Note that it is no longer relevant whether the specific data are readily accessible.) But it will then amend the DPA98 to limit the Data Subject's access rights (to be informed about such data, to be given a description of it, to have it communicated to him/her, etc.) unless the Subject's request "contains a description of the data".

It would seem that a student Data Subject could therefore request information from an unstructured tutorial file, provided that the student could give "a description of the data".

Public authorities are allowed to refuse to comply with such a request if it is too expensive to do so. However "too expensive" has now been defined by the Secretary of State as "costing more than £500 of staff time in assembling the information". This does not include any time required for determining what information is held, or making decisions about the release of the data, and is therefore unlikely to afford a reason for not complying with a Data Subject access request.

5. Confidential references

Annex 6 contains the draft JISC Code of Practice in relation to confidential references, which summarises the impact of the Act.

5.1 References given by the University

Where a reference is written by [an employee of] the University, to a party outside the University, a Data Subject does not have the right to seek a copy from the University. However, the Data Subject may seek to obtain a copy from the receiving party. There is a general duty of care in the writing of references, whether they relate to University employees or students, and we recommend that the University should therefore give guidance to its employees on the writing of references on its behalf as to acceptable form and content. Some such comments are contained within Annex 7 to this report (which is a proposed, but not yet complete, guidance document to University staff concerning all aspects of manual data). Ideally, fuller guidance should be provided to staff who, for example, do not feel that an applicant is suited to the job/course on appropriate avenues of action. An example of such guidance may be found on the University of Sussex web pages at www.susx.ac.uk/Units/dpo .

5.2 References received by the University

The University is obliged to respond to a legitimate Data Subject access request by giving "a description of" the personal data held on the Data Subject, but that description can be broad. However in addition the Data Subject is, in general, entitled to have communicated to him/her the "information constituting the personal data" and any available information on the source of the data. Confidential references received by the University are not exempt from the Data Subject's right of access. However the University must consider any potential breach of confidence of a third party. The draft Code of Practice (Annex 6) says

"Information need not be provided in response to a subject access request if the release of this information would identify a third party unless:

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

(We believe that the third of these exemptions would rarely apply.)

Although the identity of a referee would obviously be revealed by supplying the entire reference, the Data Protection Commissioner has said that the University is obliged (a) to determine whether the referee consents to have a copy given to the Data Subject, and (b) to seek to provide a copy of as much of the reference as can be given without disclosing the identity of the referee.

However, it is important to note the actual wording of the Act, in which the relevant question is whether the access request can be complied with without "disclosing information relating to another individual who can be identified from that information". Thus even if the identity of the referee were already known to the Data Subject, the University should not supply information from which the identity of the referee can be identified (unless one of the exemptions listed earlier applies).

The Working Party also notes that "obligation" (b) above is at variance with the view stated by the Government Minister (Lord Falconer of Thoroton) during the Committee stage of the Bill:
"We [the Government] believe that normally, unless there is a special situation, [the duty of confidentiality] would mean that references from another person to the data controller would not have to be disclosed…."

At this point we must therefore conclude that the legal position is uncertain. The University must fulfil its duty of confidentiality to the third party (referee), but must seriously consider whether disclosure of part(s) of a reference is possible.

The draft JISC Code of Practice in Annex 6 states: "HE and FE institutions may not refuse to disclose references received in confidence from third parties without providing reasons." However, this is not a requirement of the Act, nor is it repeated in other guidance. We therefore believe it should not be stated in this way in the Code of Practice (unless it becomes a requirement as a result of the Freedom of Information Act).

The Working Party considered a carefully detailed argument that a reference received in the form of a written letter might fall outside the definition of data "recorded in a relevant filing system", and therefore not be covered by the Act at all. The Working Party was not competent to decide whether this argument would be successful in a Court. However it would be safest, in determining University policy on the retention of Confidential References, not to assume that the argument would be successful. In any case, this argument would not apply to references received by email, or references received by telephone and recorded by a University employee.

The Working Party recommends that the University must first decide as a matter of policy whether it wishes to continue to seek confidential references in relation to

- undergraduate student applicants [a College matter]
- graduate student applicants [a University matter]
- applicants for employment.

Some organisations adopt a policy that all references written by their employees are to be "open". UCAS, in relation to references for undergraduate student applicants, has stated that its policy is that UCAS references in future will be "open". However the working party believes that the University will wish to

continue to seek confidential references in relation to prospective employees, and probably also in relation to undergraduate applicants. The following paragraphs assume that this is the University's wish.

When faced with a subject access request to see a copy of a reference, the University will be obliged to consider whether there is a duty of confidentiality to the referee or other third parties, what steps have been taken to try and obtain consent, and whether the referee has expressly refused to give their permission for the information to be made available.

The working party feels that it would be ineffective to claim that silence on the part of the referee will be taken to imply non-consent to the disclosure of the reference, even if a statement of this presumption were included in the request to the referee. We therefore recommend that in seeking confidential references, the University should make it its policy to

- inform the referee of its policy in relation to references
- ask the referee to state unequivocally whether or not he/she objects to the reference being released to the data subject in the event of a subject access request
- provide the referee with a simple way to state that they do not consent to the disclosure (for example a tick box) and
- make a clear statement that "no response" will be taken to imply consent to disclosure.

Such a policy would not prevent a referee from writing an "open" reference, but would reduce the administrative burden consequent on a Data Subject access request in cases where the data included confidential references. Also (as mentioned at the start) the existence of a clear policy will be of value to the University in defending its decisions, if challenged.

5.3 Internal references

Where a confidential reference is supplied within the University by one employee concerning another, then it is afforded the same protection under the Data Protection Act as a confidential reference from outside the University, and should be dealt with in a similar way (i.e. the writer should be asked to signify a wish for confidentiality). The matter is covered by section 7(4) of the Act, and a further defence also exists under paragraph 1 of Schedule 7. It is understood that the Data Protection Commissioner concurs in this view.

5.4 Archived references

Some have argued that the duty of confidentiality to referees does not end with their death. This argument is based on the fact that in defining "Personal Data" the Act refers to a "living individual", whereas in defining the duty of confidentiality to referees it refers only to "an individual". Even if this argument is accepted, it would not be reasonable to continue that duty indefinitely into the future. The Working Party concludes that judgements will have to be made in individual cases, but that such judgements should be made in the context of a University policy on weeding, retention and archival (see section 7).

6. Research

The provisions of the Act in relation to research activities are summarised in Annex 5. Certain exemptions from the Act may be claimed if the following two safeguards are met:

- the data are not processed to support measures or decisions with respect to particular individuals ***and***
- that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

If these safeguards are met, then the following exemptions apply to data processed for research purposes:

- personal data can be used for research even if they were not originally obtained for that purpose
- the data can be retained indefinitely
- subject access rights do not apply if the research results are not made public in a form which identifies the research subjects
- certain disclosures of the data can be made — to anyone in connection with research purposes, to the data subject, or with the consent of the data subject

These exemptions are limited in scope, and the Data Protection Principles still apply to research data, except data for "Historical research", which are further exempted from most of the provisions of the Act.

The "Data Protection (Processing of Sensitive Personal Data) Order 2000" allows Sensitive Personal Data to be processed for research purposes in the same way.

It is important that the University provides clear guidance to its employees and students on the obligations which the Act imposes on them even given the research exemptions. (If processing is carried out which does cause a Data Subject significant damage or distress, then the Data Subject can seek compensation in the Courts.) A draft of such guidance is presented in Annex 5.

7. Records management policy - weeding, retention and archival

It is important for the University to decide its policy on the weeding, retention, and transfer to archives of Personal Data. A policy is required for both long term and short term reasons. The long term issue is that Data Protection Principle 5 states that "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes". (This principle was in the 1984 Act, but now applies to "Manual records" as well.). However, some retention is necessary to meet legal requirements and to support good personnel management practice. At least 7 years' retention would be sensible as the normal limitation period for contract and tort (e.g. negligence) claims is 6 years; however longer limitation periods can occasionally apply.

The University also has archives which support historical research, and the Working Party believes that the University should wish these archives to continue to be a valuable resource for historical research. However, it would not be sensible, nor is there space, to transfer all records into the archives, so there is a need to determine what should be archived.

7.1 Policy on Manual records

It is necessary for the University to weed its manual records where necessary, so that they conform to the requirements of the Act (for example, Data Protection principles 3, 4 and 5, as listed in Annex 2) when the transitional exemption for manual records ceases in October 2001. At that date Data Subjects will be able to submit access requests related to such manual data, and it is therefore also important that the University has proper records of its Manual personal data. The Working Party believes that the effort required to carry out the weeding, archival and cataloguing processes will be substantial, and that they will be time consuming. It is therefore urgent to define a retention and archival policy, and to give further instructions to departments on the tasks which must be carried out in relation to Manual records. This also has training implications, as discussed in section 15.5.

A proposed guidance document to University staff, including paragraphs suggesting certain aspects of policy, has been prepared by the Personnel Division and is presented in Annex 7. This is work in progress. The working party recommends that the University Data Protection Officer and his Administrative Officer work with Personnel Division to bring forward an agreed guidance document for adoption as University policy.

7.2 Archival policy

The Working Party agrees with the Deputy Keeper of the University Archives that the University should not contemplate the destruction of the student and staff records which have already been transferred to the University archives from central bodies, departments and faculties over the last 20 years. As existing University policy, this material is already and necessarily restricted to researchers in view of its sensitivity (personal information is closed for 80 years) and nothing is added to or subtracted from it to ensure authenticity and integrity.

There is however a broader issue, namely that there may be other series of data currently in use which could be historically valuable and should at the end of their administrative life be transferred to the archives. This is an issue of archival policy which goes beyond the question of Personal Data and the Act.

7.3 The need for Records Management and Audit

The Working Party concurs with the view that both

- the formulation of policy on record retention and archival (of Personal and other Data, and taking into account legal requirements and good practice), and
- administration of the weeding and archival processes,

would be greatly assisted by an administrative regime which includes modern records management. This means the self-conscious audit and appraisal of records by their users, and the assignment to records of categories of relevance and currency for administrative purposes.

An assessment might find, for example, that the contents of a filing system are current for 5 years from creation, semi-current for 5 years thereafter, and may subsequently be transferred to archives (or shredded) as non-current records. The categories – current, semi-current and non-current – would take into account all legal requirements for retention or disposal, including the terms of the Data Protection Act. Lists of record series and the retention requirements for each ('Records Retention Schedules') would be drawn up for each division/department of the University.

This process would ensure that the request, already made by the Registrary in August 1998, for the Chairs of Faculty Boards and Heads of Departments to review local policies on record retention was appropriately enacted. It is important for this to occur before October 2001.

A further point is that, both to ensure that the University's holdings of Data conform to the Data Protection Act and other legislative requirements, and also to prepare to handle Data Subject requests related to manual Data from October 2001 onwards, a survey of personal data needs to be undertaken throughout the University (see section 15.4).

The Working Party therefore recommends the University to allocate appropriate resources to these tasks (giving advice on retention policy, and carrying out assessment and audit) in the near future. A request to appoint qualified record managers to assist in the audit process was agreed to by the Registrary in principle in 1999, but has not been taken further yet.

8. Exchange of Data between Colleges and the University

The Working Party believes that the Colleges and the University, being legally separate institutions, must be separate Data Controllers. It is therefore necessary to arrange that the exchange of information between them for their joint operation is as free as possible.

It is important to avoid relying on consent which can subsequently be withdrawn. The Working Party therefore recommends (as detailed in Annex 8) that offers of places to students in future are made conditional on the acceptance of the terms of a Matriculation Declaration, which includes irrevocable consent to the processing by Colleges and the University of Personal Data and Sensitive Personal Data "for the proper purposes of those institutions".

The draft matriculation declaration contained in Annex 8 incorporates a clause which makes students acknowledge their own responsibility under the Act for any Personal Data which they process. Annex 8 also contains the proposed wording of a statement to be made with the offer of a place, to explain the requirement to agree the matriculation declaration.

We recommend that an appropriate joint College and University body takes forward this proposal.

Because the Colleges and University will be separate Data Controllers, any exercise by a Data Subject of his/her rights – for example Data Subject access requests, or requests to cease processing for the purposes of direct marketing – will by default need to be made independently to the University and to (usually only one) College.

However, the use of the proposed joint matriculation declaration may create an impression that the College(s) and University are a single organisation. The University and Colleges should therefore either

- explain clearly to all students that they are separate Data Controllers, and must therefore be approached separately by Data Subjects when required (this is the preferred approach); or
- agree to a procedure for exchanging details of Data Subject requests and instructions, so that a request to either the University or a College is communicated to both. However, if such a procedure were adopted, it would be necessary to explain clearly to all students that if they, as Data Subjects, wished to make a request of only one or the other body (for example, to stop direct marketing by only one of the bodies), then they must clearly explain that when making their request.

The Working Party recommends that this matter be considered further by an appropriate joint College and University body.

8.1 Supervision Reports

Although supervision reports are formally the responsibility of Colleges, they are part of the joint teaching process, and are so considered by the QAA in Teaching Quality Assessments. It would also be desirable for the University and Colleges to adopt a consistent approach in their policies on Supervision reports, confidential references, examiners' reports and feedback to schools.

The points made in relation to confidential references in section 5.2, and the options described in that section, may be relevant to supervision reports, although it is less clear that there is a duty of confidence to the authors of supervision reports.

9. Examinations and publication of results

Examination "marks and other information processed by the data controller" fall within the scope of the Act. Information recorded on scripts by candidates during an examination is exempt from subject access, but information recorded on scripts by anyone else (e.g. an examiner) is not.

'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 counted as 'examinations'.

Where a Data Subject makes an access request in relation to examination marks or results, the time to respond is extended to either five months from the date of request, or forty days from the announcement of the examination results, whichever is earlier. If other data are recorded with marks from individual papers (either on scripts or as computer or manual files), subjects may request access to this personal data, albeit with an extended time for the University to supply it.

The Working Party believes that the specific provisions of the Act in relation to "automated decision making" are not relevant to any examination process in this University, because all examination results arise from deliberations by examiners.

9.1 Undergraduate examinations

The draft JISC code of practice in relation to examinations is presented in Annex 9. This gives a full explanation of the effects of the Act. The working party recommends that that document, and the following comments, be brought to the notice of the Education Committee of the General Board, which should be asked to agree a University policy on appropriate examination marking processes in the light of the Act.

The Act states that institutions are not obliged to provide examination candidates with either original scripts or copies of the scripts. However, examiners' comments and marks are covered by the 1998 Act, whether they are made on the script or in any other form that allows them to be held and applied to the original script (e.g. in a coded table) – assuming that they are retained in a "relevant filing system". Therefore a data subject has the right to request that a copy or summary "in intelligible form" of such comments be provided.

In most cases, we believe that it is unlikely that the University could argue that revealing the examiner's comments or marks would be "supplying information from which the identity of the examiner can be identified". Even if this were argued, it would then be necessary to ask the examiner whether s/he would consent to its release, and then to consider whether it is reasonable in all the circumstances to release the information without consent.

Therefore two matters should be considered; first, how to reduce the number of occasions on which candidates feel it necessary to make an access request, and second, how to provide the information at as little cost in time as possible.

In relation to the first point, we note that the amount of feedback to students of exam marks has increased in recent years, and recommend that the provision of as much information as possible should continue to be encouraged, since the more this is done the less likely it is that a candidate will feel it necessary to make a Data Subject Access request.

In relation to the second point, a faculty may (for reasons of the effort required) not wish by default to supply full information to candidates, but would be able to supply further information if specifically asked. In this case the appropriate procedure for making an access request to the faculty should be clearly communicated to the candidates, in order to avoid unnecessary Data Subject access requests to the UDPO.

In order to facilitate compliance with a Data Subject access request, a practice has been proposed in some other Universities of asking examiners to make their comments in a separate book either instead of, or in

addition to, the script itself. This seems preferable to the suggestion in Annex 9 that tear off comment sheets be provided in examination script booklets.

A time limit should be set after which detailed marks should be destroyed – this is one aspect of a retention policy.

The University must advise examiners of the provisions of the Act in relation to examination marks and other retained data, and remind them to ensure that all comments are appropriate. Annex 9 contains proposals that such guidance should be provided to internal and external examiners.

9.2 Postgraduate examinations

The language of Annex 9 is predominantly suggestive of undergraduate examinations. However, examiners' reports on research degrees are also covered by the Act. We believe that the issues arising in this connection are very similar to those which arise in relation to confidential references (section 5.2), and that similar policy decisions must be taken. Thus we believe that even if the identity of the examiner is already known to the Data Subject, the University should not supply information from which the identity of the examiner can be identified, unless (as before)

- the examiner has given his/her consent, or;
- it is reasonable in all the circumstances to release the information without consent.

However, the University is still obliged to provide as much information as can be provided from an examiner's report without revealing the identity of the examiner concerned.

We therefore recommend that the University, through the Board of Graduate Studies (in consultation with the University Data Protection Officer) should define its policy in relation to the confidentiality of examiners' reports for postgraduate qualifications. As mentioned before, the existence of a clear policy will be of value to the University in defending its decisions, if challenged.

Because of the obligation to seek consent, a policy that all examiners' reports are by default confidential would result in an administrative problem in the event of a Data Subject access request. We therefore recommend that the policy should be similar to that proposed for soliciting confidential references, namely that in soliciting examiners' reports, the University should

- inform examiners of its policy in relation to confidentiality of reports
- ask the examiner to state unequivocally whether or not he/she objects to the report being released to the data subject in the event of a subject access request
- provide the examiner with a simple way to state that they do not consent to the disclosure (for example a tick box) and
- make a clear statement that "no response" will be taken to imply consent to disclosure.

9.3 Publication of results

Annex 9 recommends that the University 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.

The ODPC has recently advised the University of Wales (which publishes its degree results on public noticeboards and in the relevant regional newspaper) that, providing such publication is done in a way which does not enable individual students to be contacted, then it does not breach the DPA. We believe that if the University's degree publication methods (on noticeboards and in the printed Reporter) are explained to students prior to matriculation then students can be required to consent to such publication as

part of a matriculation declaration (see annex 8), and that this would be a reasonable policy of the University – it is after all what has happened for every student to date.

Annex 9 contains suggestions for alternatives to current methods of degree result publication. Because of the preceding recommendations, the Working Party does not believe that these alternatives need to be considered.

Annex 9 recommends that the University should not:

- display results outside its 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.

The Working Party commends these recommendations to the University, noting that there is a difference between withholding results (which the Act makes impossible) and withholding a degree (which is not affected by the Act).

The particular issue raised by the prohibition of Internet publication is that the Reporter has, recently, been put onto the Internet; see section 17 for further comments concerning this. The UDPO has, to date, prevented the main Class Lists special issue of Reporter being put on the web. The working party (Dr Reid dissenting) believes that this prohibition should continue, pending receipt and consideration of the further advice, which (in section 17) we recommend should be sought on this matter.

10. Security policy

The Act requires the University to have "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". This requires both electronic security and physical security. A security policy and procedures are prerequisites for the University's Notification (registration) with the Data Protection Commissioner in October 2001.

A comprehensive discussion of security issues, and draft guidance, are contained in the draft JISC Code of Practice in Annex 10. It covers appropriate electronic security practices; training and guidance for employees and students; recommended security procedures for visitors to University sites (including contractors, vendors and suppliers); accompanying guidance to employees and students to challenge, or report to security, unauthorised individuals found in relevant areas; security issues for staff wishing to access personal data abroad.

As far as the Working Party is aware, no one body within the University has been responsible for all these different aspects of security. However, as part of the work on Information Strategy, an information security group has been formed, with representation from the Management Information Services Division, the Computing Service, the Data Protection Office, Colleges and the General Board. We therefore recommend that Annex 10 be forwarded to this information security group, together with the University Security Adviser, and that this group be asked to produce a data security policy, preferably modelled on Annex 10, for adoption by the University. The group should seek comments from the Personnel Division.

11. Implications for the University's computing services

The Act has several implications for computing systems within the University, and these affect both the central Computing Service and the computing systems in departments and other University institutions. One of the issues is that any information placed on the World Wide Web (WWW) is readable outside the European Economic Area, and the Act forbids this without the consent of each Data Subject concerned.

Annex 11 contains the draft JISC Code of Practice on "The Internet and World Wide Web". The University computing service has already had a group working on the implications of the Act, and its conclusions are in line with those of Annex 11. The inclusion of individual entries on the WWW-searchable phone/email list is already being made subject to consent.

However it is clear that, within the University, the provision of a phone or email account to any individual is on the basis that it is required for University purposes. Therefore full email address lists should still be made available internally within the University, in the same way as the University telephone directory, on the grounds that they are necessary for the purposes of legitimate interests pursued by the University.

12. CCTV systems

The Act applies to CCTV systems. The draft JISC Code of Practice in relation to CCTV systems is given in Annex 12, but does not contain much information. The Data Protection Commissioner's code of practice, referred to in Annex 12, has been withdrawn for revision.

The Working Party consulted the University Security Adviser, who explained that the University already conforms to the relevant British Standard, 7958:1999, "CCTV Code of Practice". He does not believe that new facilities or procedures will be required as a result of the new Act.

If any departments or other University institutions install local CCTV systems, it is essential that they consult the University Security Adviser to ensure that they conform to all legal requirements, including those of the Data Protection Act.

13. Alumni Activities, Direct marketing and Fundraising

The Act has many implications for Alumni activities, direct marketing and fundraising.

Direct marketing is defined in the Act as ‘the communications (by whatever means) of any advertising or marketing material which is directed to particular individuals’. This is a broad definition, that is not restricted to commercial products or offering goods for sale. The Data Protection Commissioner takes the view that the term direct marketing applies not just to the offer for sale of goods and services, but also the promotion of an organisation’s aims and ideals, including appeals for funds or support.

Therefore, both alumni/development activities and the inclusion of advertising inserts in newsletters are direct marketing.

As the Act gives data subjects the right to prevent the processing of their data for the purposes of direct marketing, whenever direct marketing is done, there must be a mechanism for maintaining an opt-out list. Special regulations apply to telephone calls — it is unlawful to make unsolicited calls to numbers who have registered with the official ‘stop list’, currently the Telephone Preference Service.

Specific guidance on the implications of the Act for alumni activities was obtained at a meeting in January 2000, which is included as Annex 13. It was established that alumni might ‘reasonably expect’ Alumni Offices to process their data for various purposes (listed in the document), which do not therefore require explicit ‘positive’ consent.

However, an opportunity must be provided for recipients to say that they do not want future mailings. Therefore a mailing opt-out list needs to be maintained – either a single joint College / University list, or an arrangement for pooling opt-out requests. All future telephone calling must conform to the requirement to check with the Telephone Preference Service first. We recommend that the Development Office maintains an opt-out list for the University, on behalf of the University Data Protection Officer.

The exchange of data with overseas Alumni offices is acceptable to the Data Protection Commissioner's office, subject to explicit confidentiality agreements, notification of this intended purpose to alumni, and an opt-out provision.

The University development office is aware of this guidance and it must continue to seek up-to-date guidance on the implications of the Act, in conjunction with the UDPO.

Since the operation of the opt-out provisions must operate across the whole University, on the basis of a single Data Subject opt-out request, it will be necessary to maintain a list of all alumni mailing and direct marketing activities. It will also be necessary to institute a procedure by which the departments notify the Development Office (as holder of the opt-out list) of any opt-out requests, and vice versa.

The Working Party recommends that every department or other institution within the University should be made aware of these implications of the Act for alumni activities and direct marketing, and required to provide information to the University Data Protection Officer about what alumni databases are held.

It is believed that some departments have existing arrangements in which Alumni names are passed to third parties, not under University control, for alumni fundraising purposes. Such arrangements would be very much affected by the Act, and may be of particular concern to the University. Departments should be made aware of this, and asked to provide information about any such activities to the University Data Protection Officer.

14. The University Card and other access systems

The proposed University Card is a new purpose, introduced after October 1998. Any data held in connection with it is therefore immediately subject to the full provisions of the Act. In the pilot Card project, it is possible to use consent as the basis for processing. However, if the Card is to become the essential device for achieving certain University (including department) purposes, such as access control, then consent which may not be given, or may be withdrawn, is not a satisfactory basis for the processing.

Provided the processing associated with Card data is suitably limited, the University may reasonably take the view that this processing is "necessary for the purposes of legitimate interests pursued by the data controller", and this is the basis which we recommend. In discussion with the University Data Protection Officer, the University Card management committee has produced a statement of the purposes to which Card data may be put.

We note that the University and Assistants Joint Board has recently reminded all departments in the University that access control systems should not be used for monitoring of staff timekeeping, and that if such monitoring were to be used, affected staff would have to be informed in advance.

It is still necessary (under the Fair Processing code) to inform Data Subjects of the uses to which the data will be put.

15. Management and administration within the University

15.1 Notification (Registration)

The "Registration" procedure under the 1984 Act has been replaced by a **Notification** procedure under the new Act. The Data Protection Commissioner has made it clear that she does not wish to have large numbers of separate notifications from a single organisation (a change from previous arrangements). However, the Working Party concluded that it will be both desirable and possible to retain separate notifications for the University, UCLES and the CUP. These three organisations need to lodge their notifications by (different but nearby) dates in Autumn 2001. The University Data Protection Officer is in contact with UCLES and CUP to ensure that the joint aim of separate notifications is pursued effectively by the three organisations.

A standard template for University notifications has been prepared by the Commissioner, although not published, and it seems (from a draft version which the UDPO has seen) that notification will not pose any particular problems for the University.

The Colleges, as legally separate bodies, will each require separate notifications. The proposed template for University notifications is likely to serve the needs of Colleges too.

Separate organisations such as CUTS (Cambridge University Technical Services Ltd), CMIL (Cambridge Manufacturing Industry Links Ltd) and (perhaps) the Cambridge Foundation, will have to handle their own registrations.

15.2 Subject Access Requests – the need for a central register

Currently, in response to a subject access request, potential data holders are contacted and asked to either supply the data required by the Act or confirm that they do not hold any such data. This is administered through a network of local Data Protection Officers. There is no central register of where specific information is held; the current system mirrors the 1984 Act registration regime which records general classes of purposes for which data are held.

This system has proved adequate for requests under the 1984 Act, which are restricted to data automatically processed by reference to the data subject. However, even under the 1984 Act requirements, it can be difficult to comply with requests within the 40 days specified by law, as time is taken identifying where the required data are held, and the system is very dependent on the local Data Protection Officer.

The 1998 Act extends the scope of data enormously with the inclusion of manual records (this will extend still further when the Freedom of Information legislation amends the 1998 Act).

The system of handling requests for the 1998 Act must be able to provide an increased amount of information within 40 days. We therefore propose that the UDPO must maintain a central register of personal data. The information in this central register must initially be provided by a records audit, as described in the following subsection. It must then be kept up to date; this will require all departments of the University to continue to monitor and report to the UDPO all new uses of personal data.

15.3 Records audit

The Working Party believes that in order for the University to operate a workable Data Subject Access Request system, and also in order to ensure compliance with the Act in general, there must be an audit of

all Personal Data held in the University. In conjunction with the audit, guidance (detailing both mandatory requirements and good practice) should be provided to data holders on collection, storage and disposal of records. Compliance with the Data Protection Principles could then be ensured.

The specific audit of alumni databases and direct marketing activities mentioned in section 13 must be included within this general audit.

As a precursor to the auditing process, definitions of terms such as 'relevant filing system' must be provided to those carrying out the audits.

15.4 Ensuring continuing compliance with the Act

All data, including, from October 2001, Manual Data, must be processed following the data protection principles set out in the Act. The University must ensure that these principles are applied efficiently and effectively to the data it controls. The principles require that data are (for example) relevant, accurate, not excessive and not kept longer than necessary. Clearly, there may be administrative and cost savings in following these principles.

Currently, advice on the Act is issued from the University Data Protection Officer. However, compliance with the law is not assessed, and there is currently no assurance that data are processed lawfully. Note that unlawful processing includes any breach of statutory provisions or common law, and not only the Data Protection Act.

The obligation on the University to ensure compliance with the law means that an appropriate monitoring process (internal audit) should be put in place. This might take the form of a programme in which all departments and institutions within the University are either visited, or asked to respond to a set of review questions, in turn. The Working Party suggest that the University Data Protection Officer be asked to advise on the resource implications of this process.

Because of the work required to prepare for the ending of the transitional provisions in October 2001, the working party acknowledges that this is unlikely to be feasible until after that date.

15.5 Training

Before the 1998 Act can be implemented in the University, following the ending of transitional exemptions in October 2001, there will need to be an extensive programme of training. This training will need to be of two types:

1. **Departmental Data Protection Officers (DDPO)**

   Training for this group should provide detailed guidance on the implementation of the Act within the department dealing with policy and practical issues. The training should enable the DDPO to be responsible for the implementation of the Act within that department, and to be the first port of call for members of the department having queries.

2. All relevant members of staff, both academic and non-academic

   Training for this group should provide information as to individual responsibilities under the Act, particularly in complying with the Data Protection Principles, and good practice on the handling of personal data.

The provision of training across the University will need careful planning. It is unlikely that this will be able to be resourced from within the Data Protection Office and external trainers will therefore need to be brought in to work with existing staff. The University Data Protection Officer has already been invited to give a number talks to groups within the University to explain the background and implications of the new Act and these have all been well received. However, this approach would be impractical across the whole of the University given the time it would take to visit all departments. The University Data Protection Officer will be having discussions with the Personnel Division about the best way of delivering this level of training and incorporating data protection issues in the Induction Courses for new staff. The Working Party feel that training is a key issue in meeting the requirements of the new Act and wish to alert the Council to the cost implications of this training.

15.6 Guidance

As mentioned above, it is essential that guidance be provided to all departments and institutions within the University. The Working Party has helped the University Data Protection Officer to draft an initial guidance document, and recommends that further more detailed guidance be assembled as soon as possible.

Guidance must also be provided to employees on their rights, as mentioned in section 2.5, and on the procedures to be followed to make a Data Subject access request. Annex 7 provides a basis for this guidance, and also advice on manual records weeding, archival and cataloguing (as mentioned in section 7.1).

Guidance should be provided to employees on writing references, as recommended in section 5.

16. Student Societies

Under the 1984 DPA, most societies were exempt from the Act provided certain conditions were met. This exemption has not been carried forward to the 1998 DPA.

Student societies are not included in the University's registration under Data Protection Act because they are considered to be separate legal entities and the University does not control their data processing.

Therefore students are themselves responsible for the protection of any data that they process outside the control and responsibility of the University. This includes data processed for Student Societies, including CUSU. However, these may be exempt from the notification provisions as 'not for profit organisations' but this is a matter for the society to check directly with the ODPC.

Students and Student societies will need to comply with the data protection principles so it will be important that they are informed of their obligations. The DPWP suggest that the Junior Proctor, in consultation with the University Data Protection Officer, should issue guidance to student societies regarding their need to comply with the Act. Although some societies may have been processing personal data on 23 October 1998, and can therefore take advantage of the transitional provisions of the 1998 Act, others will not meet this requirement and therefore will need to comply with the 1998 Act immediately.

17. Publication of Reporter on the Internet

The Reporter is published as a newspaper, and contains many items which relate to specific individuals, of which examination and degree results are one example. The practice has recently started of putting the Reporter onto the Internet.

The UDPO should seek advice on whether the publication of the Reporter is covered by section 32 of the DPA, which relates to the processing of journalistic material (see sec. 2.4), and what restrictions might exist in relation to publication on the Internet. If the advice is that publication on the internet is contrary to the DPA, then the working party recommends that internet access to the Reporter should be restricted, perhaps using password protection. This would avoid the risk that an objection would be raised to publication of personal data on the Internet.

18. References concerning the DPA98

[1] "The Data Protection Act 1998 reprinted incorporating corrections 1999". (The Stationery Office Ltd.)
[2] "The Data Protection Act 1998 - An Introduction". (The Office of the Data Protection Registrar.)
[3] "The Data Protection Act 1998 - JISC Senior Management Briefing Paper 9". (JISC)
[4] "Data Protection Act 1998" - Memo from Registrary and Secretary General as annex to DB-L/492/2, 10 August 98.
[5] "Differences between the 1984 and 1998 Data Protection Acts affecting the University of Cambridge - Rachel Shapton, Dec 99.
[6] "The Data Protection Act 1998: Tutorial Files". Paper by Dr G A Reid. 19 Jun 1999.
[7] "The Data Protection Act 1998: Confidential References". Paper by Dr G A Reid. 24 Jan 2000.
[8] Document concerning CCTV use and the DPA84. Received from John Heppleston, University Security Adviser, 13 Jan 2000.
[9] "University of Cambridge, Security, Administrative and Operational Procedures for University Security Staff", S/SEC/COPS94/582, 24 March 99.
[10] Article from THES, 14 Jan 2000, p8.
[11] The (draft) Freedom of Information (FoI) Bill: http://www.parliament.the-stationery-office.co.uk/pa/pabills.htm
[12] 'Preparing for the new Act' at http://www.dataprotection.gov.uk/prepare.htm.

19. Collected recommendations

[sec 2.5] The 'purposes' for which data is to be processed should be defined as broadly as is reasonable to the Data Subject. It is believed that the proposed standard template from the ODPC will serve this purpose.

[sec 2.5, 15.7] All University Employees and Students should be made aware that any requests for access to data should be referred to the University Data Protection Officer, who will administer this process.

[sec 3] Data Subject consent should only be sought in cases where the processing is not "necessary for the purposes of legitimate interests pursued by the University". In such cases, provision must be made for ceasing the processing if consent is not given, or is subsequently withdrawn.

[sec 4] Members of the University should be advised to assume that any filing system intended to contain accessible information about living individuals is a "relevant filing system" within the scope of the Act. Cases in which there is real uncertainty should be discussed with the University Data Protection Officer.

[sec 4] Restructuring of filing systems to get around the Data Protection legislation should be strongly discouraged.

[sec 5.1] the University should give guidance to its employees on the writing of references on its behalf, as to acceptable form and content.

[sec 5.2] the University must decide as a matter of policy whether it wishes to continue to seek confidential references in relation to

- undergraduate student applicants [a College matter]
- graduate student applicants [a University matter]
- applicants for employment.

[sec 5.2] if seeking confidential references, the University should adopt the procedural policy listed in section 5.2.

[sec 6] the University should provide clear guidance to its employees and students on the obligations which the Act imposes on them in connection with research activities. A draft of such guidance is presented in Annex 5.

[sec 7.1] The University should define a retention and archival policy, and give further instructions to departments on the weeding tasks which must be carried out in relation to Manual records.
… the University Data Protection Officer and his Administrative Officer should work with Personnel Division to bring forward an agreed guidance document for adoption as University policy, based on Annex 7.

[sec 7.3] the University should allocate appropriate resources to the tasks of giving advice on retention policy, and carrying out assessment and audit in the near future. In this connection, a request to appoint qualified record managers to assist in the audit process, agreed by the Registrary in principle in 1999, should be reconsidered.

[sec 8 and Annex 8] offers of places to students in future should be made conditional on the acceptance of the terms of a Matriculation Declaration, which includes irrevocable consent to the processing by Colleges and the University of Personal Data and Sensitive Personal Data "for the proper purposes of those institutions".
[sec 9.3] this matriculation declaration should explain and require students to consent to the University's standard degree publication methods (on noticeboards and in the printed Reporter) (see annex 8).

[sec 8] an appropriate joint College and University body should develop the proposals in Annex 8, and should consider how to make clear to students the separation between College and University as data controllers.

[sec 8.1] Colleges should be invited to consider the advice given in section 5.2, in relation to supervision reports and feedback to schools.

[sec 9.1] The draft JISC code of practice (Annex 9), and the contents of section 9 of the DPWP report, should be brought to the notice of the Education Committee of the General Board, which should be asked to agree a University policy on appropriate examination marking processes in the light of the Act.

[sec 9.2] the University, through the Board of Graduate Studies (in consultation with the University Data Protection Officer) should define its policy in relation to the confidentiality of examiners' reports for postgraduate qualifications. The policy should be based on that outlined in section 9.2.

[sec 9.3] The Working Party commends to the University some only of the recommendations contained in the draft JISC code of practice on examinations (annex 9) as detailed in section 9.3.

[sec 10] the recently-formed information security group, together with the University Security Adviser, and seeking comments from the Personnel Division, should produce a data security policy for adoption by the University, preferably modelled on Annex 10, the draft JISC Code of Practice on security.

[sec 13] The University development office must continue to seek up-to-date guidance on the implications of the Act, in conjunction with the UDPO.

[sec 13] the Development Office should maintain a direct marketing opt-out list for the University, on behalf of the University Data Protection Officer.

[sec 13] a procedure must be implemented by which departments notify the Development Office (as holder of the opt-out list) of any direct marketing opt-out requests, and vice versa.

[sec 13] every department or other institution within the University should be made aware of the implications of the Act for alumni activities and direct marketing (section 13), and required to provide information to the University Data Protection Officer about what alumni databases are held. Any activities in which names of alumni are passed to third parties are of particular concern, and must also be notified to the University Data Protection Officer.

[sec 15.1] Separate organisations such as CUTS, CMIL and (perhaps) the Cambridge Foundation, will have to handle their own registrations.

[sec 15.2] the University UDPO should maintain a central register of personal data in the University.

[sec 15.3] there must be an audit of all Personal Data held in the University.

[sec 15.3] guidance (detailing both mandatory requirements and good practice) should be provided to departmental data holders on collection, storage and disposal of records.

[sec 15.4] In the long term, the University should aim to set up procedures for internal audit of the processing of personal data. The University Data Protection Officer should be asked to advise on the resource implications of this process.

[sec 15.5] training must be provided for Departmental Data Protection Officers, and for all relevant members of staff, both academic and non-academic. The cost implications of this training are significant.

[sec 15.6] Guidance must be provided to employees on

- their rights and the procedures to be followed to make a Data Subject access request.
- manual records weeding, archival and cataloguing

[sec 16] the Junior Proctor, in consultation with the University Data Protection Officer, should issue guidance to student societies regarding their need to comply with the Act.

[sec 17] The UDPO should seek advice on whether the publication of the Reporter is covered by section 32 of the DPA, and what restrictions might exist in relation to publication on the Internet. If the advice is that publication on the internet is contrary to the DPA, then the working party recommends that internet access to the Reporter should be restricted, perhaps using password protection.

Annex 1 Membership of the Data Protection Working Party

Malcolm Macleod (Chairman)	Director of Research, Department of Engineering, and member of the University Council
Andrew Barling	Solicitor & Contracts Officer, Wolfson Industrial Liaison Office
Dennis Barrington-Light	University Data Protection Officer, Registry
Mary Beveridge	Secretary, Judge Institute
Jacky Cox	Deputy Keeper, University Archives
David Harris	Computer Officer, DAMTP
Tristan Jones	President, CUSU
Jean Margrie	Personnel Officer, Personnel Division
George Reid	Chairman, Bursar's Committee & Chairman of Board of Examinations
Nicholas Robinson	Director, Management Information Services Division
Rachel Shapton (Secretary)	Administrative Officer, Registry
Brian Westwood	Deputy Director, University Computing Service
Penny Wilson	Secretary, Senior Tutor's Committee
Anna Wardman	Development Office

Annex 2 A Summary of the Data Protection Act 1998

[author Rachel Shapton]

Introduction

The Data Protection Act 1998 (the 'Act') gives effect in UK law to EC Directive 95/46/EC which requires 'Member States to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing or personal data'.

The Act replaces the 1984 Data Protection Act (the '1984 Act').

The Act introduces changes in both scope and operation that affect organisations processing personal data. The 1984 act placed emphasis on the registration of data users and the interaction between the data users and the Data Protection Registrar. The 1998 Act is concerned with the substance of how data is processed, and emphasises the interaction between the data controllers (those processing the data) and the data subjects.

Some of the significant changes in the Act are:

- The Act now covers structured 'manual' or paper records as well as automated data
- The definition of data processing has been changed and is now 'compendious…, and it is difficult to envisage any action involving data which does not amount to processing'[1]
- Data which are 'sensitive' (such as ethnic origin, membership of trade unions, etc.) are subject to additional restrictions
- Subjects' rights of access to information are extended, and can include the purposes for which information is processed, the likely recipients of the data and the sources of the information
- The process of registration of data users is replaced by one of notification of data controllers

Data Protection Principles

There are eight Data Protection Principles in the Act, and these principles apply to all personal data processed by data controllers. Controllers must comply with these principles unless certain exemptions apply. These principles are not the same as those in the 1984 Act.

1 The Data Protection Act 1998 — An Introduction, The Data Protection Registrar, October 1998

The eight principles are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in schedule 2 is met, and in the case of sensitive data, at least one of the conditions in Schedule 3 is met. *The specifying of particular conditions which must be met in order for data processing to be fair and lawful is new in the 98 Act.*
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes. *This is a change from the 1984 Act, and compatibility must be demonstrated to satisfy this principle.*
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. *Unchanged from the 1984 Act.*
4. Personal data shall be accurate and, where necessary, kept up to date. *Unchanged from the 1984 Act.*
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. *Unchanged from the 1984 Act.*
6. Personal data shall be processed in accordance with the rights of data subject under this Act. *This is a new principle introduced in the 1998 Act.*
7. Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. *This is an extension of the 1984 Act, and includes express obligations upon the Controller when data are processed by a processor on behalf of the controller.*
8. 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 a new principle introduced in the 1998 Act.*

Specific changes introduced by the Act and their implications for the University

The Data Protection Registrar has made clear her belief that at least 80% of compliance with the Act flows from complying with the 1984 Act, and there are transitional periods giving time to bring processing already underway into compliance with the Act[2].

However, there are specific changes that affect policies and procedures followed within the University.

Scope

The Act now covers not only automated records but all personal data that form part of a 'relevant filing system' (i.e. "any set of information relating to individuals…structured…in such a way that specific information relating to a particular individual is readily accessible"[3]).

Auditing all files to assess whether they meet a definition of 'relevant filing system' or are 'readily accessible' would be an enormous task. Administratively, it is probably simpler to assume that all personal data held in non-electronic form will be held so that specific information can be retrieved, and therefore will be subject to the Act.

Fair processing

Data processing must be fair and lawful, and must not take place unless at least one specified condition is met. These conditions include, for example, that the data subject has given their consent to processing or that processing is 'necessary for the purposes of legitimate interests pursued by the data controller…except where the processing is unwarranted…because of prejudice to the rights and freedoms or legitimate interests of the data subject'.

Although much of the data processing undertaken in the University could be deemed 'necessary' to its legitimate interests, obtaining consent for processing where possible is both good practice and gives the broadest protection to the University as a data controller.

'Sensitive Personal Data' are defined as personal data consisting of information as to the Data Subject's: racial or ethnic origin, political opinions, religious or similar beliefs, membership of trade unions, physical or mental health conditions, sexual life, commission or alleged commission of any offence, or proceedings for any offence committed or alleged to have been committed by the subject.

Explicit consent must usually be obtained before processing such data. Quite routine data such as personnel files and accident reports are likely to contain sensitive personal data.

The 'Fair Processing Code' specifies information that should be given to data subjects to ensure that data are fairly obtained, and 'so far as is practicable' the data subject should be given:

- The identity of the data controller
- The identity of the nominated representative
- The purpose or purposes for which the data are intended to be processed
- 'any further information which is necessary'. In deciding what is necessary to satisfy this requirement, the data controller should consider whether or not the data subjects are likely to understand the purposes of processing, the likely consequences, and particularly whether particular disclosures can be envisaged.

This information should be provided at the time of data collection.

2 http://www.open.gov.uk/dpr/cost.htm
3 Data Protection Act 1998 Part I Section 1

Given the extended scope of the Act, data capture methods will need review to ensure that consent is sought, especially for sensitive data, and that data are collected in accordance with the Fair Processing Code.

Fair processing of information obtained from third parties

Fair processing information should also be provided to subjects when data have been obtained from someone other than the data subject, unless this either involves 'disproportionate effort' or the information must be recorded to comply with a legal obligation (other than that imposed by contract). 'Disproportionate effort' is not defined, but the Registrar's guidance states that data controllers are not generally exempt from the fair processing code simply because data were not obtained directly from the subject.

Where data are received by the University from a source other than the data subject, there needs to be a mechanism of ensuring that the Fair Processing conditions are met. This includes information on current students, alumni, potential benefactors and personal data in donated archives and papers.

Access to records

A data subject is entitled to be told whether his or her personal data is being processed, and if so to be given a description of the data, the purposes for which it is being processed and to whom the data are or may be disclosed. The data subject must also be told all the information that forms the personal data in the form of a copy. This information must be supplied within forty days of receipt of the request in writing (which may include electronic transmission) and the payment of a fee.

The level of requests for access to data under the 1984 Act was quite small, but access was limited to automated records. It was apparent that most of the 'interesting' material would be held manually, and data subjects had little incentive to ask for the information available under the Act. Given the extended scope of the new Act, it could be expected that the number of requests will increase as subjects now have access to virtually all information held about them.

The Act recognises particular problems in complying with access requests where information relating to someone other than the subject can be identified, including where the information enables that individual to be identified as the source of the information. There are then only two circumstances where the controller is obliged to comply with the subject access request:

- Where the other individual has consented to the disclosure, or
- Where it is reasonable in all circumstances to comply with the request

Where the identity of the third party can be protected by anonymisation then this should be carried out and the information released. Guidance is given on responding to a request without the consent of the third party. The controller must consider any duty of confidentiality owed to the third party and any steps taken to obtain consent.

Procedures will need to be in place so that the University can provide records that may come from a variety of sources within the forty-day limit.

This may involve maintaining a central register of holders of personal data and the categories of data that are held. Establishing this register could also present an opportunity to review records held and possibly rationalise the amount of personal data held.

Confidential references

Personal data are exempt from the act when they consist of a confidential reference provided by the controller concerning education, training or appointment. This exemption is not available for such references received by the controller. To simplify complying with subject access requests it may be

prudent when requesting references to explicitly ask the referee whether they consent to release of the reference to the data subject.

Disclosure and Security

'Appropriate' security must be in place to prevent unlawful and unauthorised processing, and to prevent accidental loss or damage of data. The state of technological development, the cost of implementing measures, the harm that might result from security breaches and the reliability of staff with access to data must be taken into account when determining 'appropriate' measures. Also, where the University contracts a third party to process data (a 'data processor') this must be done under written contract and the data processor must provide guarantees in respect of security measures. Transfer of data between the separate legal entities of Colleges and the University will need to comply with the Act.

As part of the notification process with the Data Protection Commissioner, a general description of security measures taken to protect personal data must be provided.

Computer network security measures can explicitly describe the access to and use of automated data, and the 'Rules made by the Information Technology Syndicate'[4] require all users of personal data to abide by the 1984 Act. With manual records now included in the Act, a risk assessment perhaps coupled with the monitoring of data held by a central register could identify security risks and assist in identifying appropriate security measures. British Standard 7799: Information Security Management describes processes and procedures necessary to ensure information security, and working to these procedures could address the University's security requirements.

Direct Marketing

An individual is entitled to require a data controller to cease or nor to begin processing personal data relating to that individual for the purposes of direct marketing. Direct marketing is defined in the Act as meaning the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

This particularly affects approaches to alumni and potential donors. If anyone requests that they no longer receive direct marketing or fundraising information, they need only make one request to the University of Cambridge, which is the legal entity that is the data controller. If there are several groups in the University that hold personal data, and at some stage may use this information in direct marketing, all groups must be aware of, and act on, such requests.

Disclosure outside the European Economic Area (EEA)

Under principle eight, data shall not be transferred outside the EEA unless the destination country ensures adequate protection of data subjects. The European Commission can make findings that countries do, or do not, meet an adequate level of protection, although no such findings are currently in force. However, it is planned that a 'safe-harbour' arrangement will be in place between the EU and USA in autumn 1999.

It is important to note that publication on the World Wide Web will be considered a worldwide transfer of data. Currently, personal data including contact numbers and e-mail addresses are available on the Internet. Personal data such as this will require that the data subject consent to this worldwide disclosure in order to comply with the Act. Note that publishing personal data on an intranet with restricted access is not subject to principle eight. A review of data held on web pages could identify appropriate sites to disclose personal data.

4 Statutes and Ordinances of the University of Cambridge, 1998, p. 574

Examination scripts and marks

Information recorded on scripts by candidates during an examination is exempt from subject access. Where a subject access request is in relation to examination marks or results, the time to respond is extended to either five months from the date of request, or forty days from the announcement of the examination results. If data are recorded with marks from individual papers (either on scripts or as computer or manual files), subjects may request access to this personal data, albeit with an extended time for the University to supply it.

Research, History and Statistics

Data collected exclusively for research (including historical or statistical purposes) can be held indefinitely, and can be used for other research without breaching the Act. However, the data must not be processed to support decisions relating to particular individuals, and must not cause substantial damage or distress to any data subject. Subject access does not have to be given provided the results of the research or any resulting statistics do not identify data subjects.

Note also that one of the criteria for processing sensitive data is that it is for medical research, provided the processing is undertaken by a health care professional, or someone who owes a similar duty of confidentiality to the research subject.

Annex 3 Schedules 2 and 3 – conditions for processing data

SCHEDULE 2
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF ANY PERSONAL DATA

The data subject has given his consent to the processing.

The processing is necessary-
(a) for the performance of a contract to which the data subject is a party, or
(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

The processing is necessary in order to protect the vital interests of the data subject.

The processing is necessary-
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

(1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

SCHEDULE 3
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF SENSITIVE PERSONAL DATA

"Sensitive personal data" means personal data consisting of information as to-
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The data subject has given his explicit consent to the processing of the personal data.

(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
(2) The Secretary of State may by order-
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

The processing is necessary-
(a) in order to protect the vital interests of the data subject or another person, in a case where-
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

The processing-
(a) is carried out in the course of its legitimate activities by any body or association which-
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical, religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

The processing-
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

(1) The processing is necessary-

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(2) The Secretary of State may by order-
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

(1)The processing is necessary for medical purposes and is undertaken by-
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

(1) The processing-
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Annex 4 A Summary of the Transitional Provisions in the Act

[author Rachel Shapton]

"Personal data are eligible for [transitional relief]]… if they are subject to processing which was already under way immediately before 24th October 1998" [5]. The personal data themselves do not have to have been in existence in October 1998 but the processing to which they are subject must have been.

Are data eligible [for transitional relief]?

(a) The addition of a new item of data where data in that category are already held is not new processing
(b) Use of data for a closely related purpose is not new processing
(c) Disclosure of additional data to recipients who already receive new information is not new processing
(d) Use of existing data for a new purpose is new processing
(e) Disclosures to new recipients is new processing

For example, the University Card is new processing as it collects new information for a new purpose. Creating a new personnel file for a new member of staff is not new processing, as the University was processing data for personnel files on 24 October 1998.

Eligible automated data – exemptions to 23 October, 2001

Schedule 8 describes the following exemptions:

Paragraph	Exception	Exempt from:
13(1) (a) (i)	Fair Obtaining & Processing Code	Para. 2 of Part II of Schedule 1
13(1) (a) (ii)	Legitimacy of processing rules	Schedule 2
13(1) (a) (iii)	Sensitive data processing rules	Schedule 3
13(1) (b)	Controller contracts with data processors	Para. 12 of Part II of Schedule 1
13(1) (c)	Transborder transfers	Principle 8, Schedule 1 part I
13(1) (d)	Additional information provided on subject access request	Section 7(1) paras. (b), (c)(ii) and (d)
13(1) (e)	Right to prevent processing likely to cause damage or distress Right to removal from marketing list	Section 10 Section 11
13(1) (f)	Rights in relation to automatic decision making	Section 12
13(1) (g)	Claims for compensation in part only	Section 13 in part only

Paras. (a), (c) & (e) do not limit duty to process data fairly[6]

Notes:

- Until 23 October 2001, eligible automated data are not to be regarded as being 'processed' unless processing is by reference to the data subject[7]. This means that the effect of the Act during this period is restricted to the kind of data caught by the 1984 Act.

- Back-up data (processed only for replacing other data in the event of the latter being lost, destroyed or impaired) are exempt from subject access to 23 October 2001[8].

5 Schedule 8, 1 (1)
6 Schedule 8, 13 (2)
7 Schedule 8, 5

- Payrolls & accounts data are exempt from data protection principles and Parts II and III of the Act [9] to 23 October 2001.

- Mailing lists are also exempt from principles and Parts I and II to 23 October 2001.

- Exempt data can still be subject to a claim under restricted Section 13 rights (compensation for damage), which continues from 1984 Act

Manual Data

Manual data are subject to the act if they are a set of information that is structured by reference to individuals or reference to criteria relating to individuals such that specific information relating to a particular individual is readily accessible. Data must be both structured and specific to be caught by the Act.

Note however that the Freedom of Information Bill as drafted (expected to receive Royal assent in July 2000) will extend the provisions of the Data Protection Act to include unstructured data (but not unstructured personnel and employment records).

Eligible Manual Data – exemptions to 23 October, 2001

Eligible manual data are exempt from data protection principles and Parts I and II (including data subject rights). Note that section 55 still applies, so knowingly or recklessly obtaining or disclosing data without consent is an offence.

Eligible Manual Data – exemptions from 24 October 2001 – 23 October 2007

For data that were actually held on 23 October 1998, there are some further limited exemptions. These particular documents will be exempt from the requirements for legitimate processing (Schedule 2), the sensitive data controls (Schedule 3), and the general requirements that data shall be processed fairly and lawfully. They are also exempt from the following data protection principles:

- Principle 2: Data shall be obtained for specified and lawful purposes
- Principle 3: Data shall be adequate, relevant and not excessive
- Principle 4: Data shall be accurate and up to date
- Principle 5: Data shall not be kept longer than necessary

There will be rights of subject access to these records from 24 October 2001.

---

8 Schedule 8, 12
9 Schedule 8, 6

Annex 5 – Implications of the DPA98 for Research

[author Rachel Shapton]

There are certain limited exemptions from the Act for research purposes (section 33 of Part IV of the Act).

Research, which includes statistical and historical studies, can claim certain exemptions from the Act if two safeguards are met. The safeguards are that

- the data are not processed to support measures or decisions with respect to particular individuals ***and***
- the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

If these safeguards are met, then the following exemptions apply:

- personal data can be used for research even if they were not originally obtained for that purpose
- the data can be retained indefinitely
- subject access rights do not apply if the research results are not made public in a form which identifies the research subjects
- certain disclosures of the data can be made — to anyone in connection with research purposes, to the data subject, or with the consent of the data subject

Note that these exemptions are limited in scope, and the Data Protection Principles still apply to research data (except data for "Historical research" – see below). The data must have been obtained for one or more specified and lawful purposes. Its processing for the research purposes must still meet one of the conditions in Schedule 2 of the Act (see Annex 3 above); the Working Party believes that the University could reasonably take the view that processing data for research will often be "necessary for the purposes of legitimate interests pursued by the University". Alternatively, the consent of the Data Subject should be sought. The processing of Sensitive Personal Data for research, except historical or medical research (see below) requires one of the conditions in Schedule 3 of the Act (see Annex 3 above) to be met. When data collected for another purpose are used for research, the data subject should be contacted and informed of this, unless it would involve 'disproportionate effort' in which case this should be documented.

Transfers of data abroad can only take place if certain conditions are met: usually either that the subject has consented to the transfers, or the conditions of the transfer ensure that their rights and freedoms are preserved.

Historical research

"Historical research" is subject to further, significant, exemptions (Part IV of Schedule 8 of the Act); in essence only Principles 7 (appropriate security) & 8 (restricting transfer outside the EEA) apply to data processed for this purpose.

Medical Research

Sensitive data (which includes information about someone's physical or mental health) may be processed on the basis that it is ***necessary*** for medical purposes, including medical research ***and*** it is undertaken by a health professional or someone with an equivalent duty of confidentiality.

Note that the Data Protection Commissioner's view under the previous Act was that where confidential personal data derived from NHS health care is processed by researchers other that the doctor who treats

the patient, then consent should be given by the subject for this. The Commissioner's view is that where personal data are processed in breach of an obligation of confidentiality, such processing will be unlawful in the absence of consent.

Health Records

Health records (i.e. records relating to physical or mental health that have been made by on behalf of a health professional in connection with the care of that individual) are subject to specific guidance:
Health Service Circular HSC 2000/09, issued 23 March 2000
'Data Protection Act 1998, Protection and Use of Patient Information' www.doh.gov.uk/coinh.htm
and HSG(96)18 www.doh.gov.uk/dpa98

All patient records must comply with this guidance, and note that Department of Health guidance goes further than Act in some areas, and emphasises the common law duty of confidentiality that applies to all staff working for the NHS. Note also that even if data have been anonymised this does not of itself remove the duty of confidence, and data may still only be passed on for a justifiable purpose.

All research proposals involving access to patient records require clearance by the local research ethics committee.

Note that any personal data consisting of information as to the physical or mental health or condition of an individual are subject to the 'Data Protection (Subject Access Modification) (Health) Order 2000'. This is published as Statutory Instrument 2000 Number 413. This order has a number of important provisions:

- Health information is exempt from subject access if that access would be likely to cause serious harm to the individual or any other person.
- In deciding whether to provide subject access, the data controller must consult the health professional responsible for the individual's clinical care
- The data controller cannot refuse access because another individual would be identified if that third party is a health professional, *unless* serious harm to the health professional's physical or mental health would result from access being granted.

This has important implications — requests for access to any health data must be processed in consultation with health professionals. This would include information in, for example, counselling or occupational health services files and Applications Committee files.

Draft Data Protection Act 98 Research Checklist

Does the project involve personal data, i.e. relating to a living individual who can be identified from that data or other information in the possession of, or likely to come into the possession of the data controller?	*If no then the Data Protection Act 1998 (DPA 98) does not apply to the project.*
Does the project meet the definitions in the Data Protection Act 1998, i.e. for research, historical or statistical purposes?	If no, then the DPA 98 applies in full *If yes, then research exemptions may apply*
Who is the data controller for the personal data, that is the person who controls the purposes and manner of processing?	*If it is the University, you need take no further action (the University has notified that Data Protection Commissioner that it processes personal information for research purposes.)* *If the data controller is not the University (and note that Colleges are independent data controllers), you must tell this other data controller who will check whether a further notification is required.*
Check Schedule 2 and decide which condition for processing you are relying on for the project	
Is any of the data sensitive data? If so, check the conditions in schedule 3 and decide which you are relying on for your project (this in addition to a schedule 2 condition).	
Will any personal data be transferred overseas as part of the research project?	*If so, you will need to demonstrate that the transfer preserves the subject's rights and freedoms.*
Were individuals told at the time data were collected that their data would be used for research?	*If no, either arrange to have them informed of this, or if this would involve disproportionate effort you must document the reason why this is so.*
Will the results of the research be used to make any decisions about the research subjects, for example in a group with a particular medical condition will the results be used to determine subsequent treatment for a member of the Group?	*If so, no exemptions apply and the Act applies in full.*
Could the data processing being carried out result in any damage or distress to individual subjects?	*If it could, no exemptions apply and the Act applies in full.*
Will the results of the research be made public in anonymised form only?	*If so, subject access rights do not apply to the personal data used in research.*

Annex 6 - Draft JISC Code of Practice on Confidential References

[author Andrew Charlesworth]

References given by HE and FE institutions

Confidential references given by the Data Controller, including those written by an individual acting on his behalf, are exempt from the right of access. Thus, references written by members of an institution's staff in the performance of their institutional duties 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 the Data Controller are not exempt from the right of access, but consideration must be given to any potential breach of confidence of a third party. Information need not be provided in response to a subject access request if the release of this information would identify a third party unless:

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

- HE and FE institutions, when faced with the question of subject access to a reference received in confidence from a third party, must consider whether there is a duty of confidentiality to the third party, what steps have been taken to try and obtain consent, and whether the third party has expressly refused to give their permission for the information to be made available.

- 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:

- 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 staff writing references on their behalf as to acceptable form and content;
- providing advice to staff who do not feel that an applicant is suited to the job/course on appropriate avenues of action.

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 another part of the same institution, or indeed to be used by an individual in the same department. It would be incongruous

if, because the reference remained within the overall Data Controller, the Institution, it were to be somehow exempted from all 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 a third party.

Annex 7 - Draft Guidance and Policy statement to University Staff

[author Jean Margrie]

DATA PROTECTION ACT 1998 – INFORMATION HELD ON STAFF

Introduction

The Data Protection Act 1998 came into force in March 2000. It repeals the 1984 Data Protection Legislation and aims further to harmonise data protection law throughout Europe. It also addresses fundamental issues of individual rights to privacy and freedom of information.
Under the Act, personal data must be processed following the Data Protection Principles so that data are:

1. processed fairly and lawfully and only if certain conditions are met
2. obtained for specified and lawful purposes
3. adequate, relevant and not excessive
4. accurate and where necessary kept up-to-date
5. not be kept for longer than necessary
6. processed in accordance with the rights of data subjects
7. kept secure
8. not to be transferred abroad unless to countries with adequate data protection laws

Definitions

'Data' is information processed automatically or recorded with the intention
that it should be processed automatically. It is also information recorded as part of a 'relevant filing system' – information structured so that it can be readily attributed to a particular individual. Manual data, card files, microfiches and other paper files are included here.

'Personal data' are data that relate to a living, identifiable individual.

'Data subject' is an individual who is the subject of personal data.

'Sensitive personal data' are
(a) racial or ethnic origin
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) membership of a trade union
(e) physical or mental health or condition
(f) sexual life
(g) the commission or alleged commission of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

'Data controller' is a person or organisation who controls the purposes and manner in which data are processed. For the purposes of holding and processing staff data in the University, the University of Cambridge is the data controller, and the nominated representative of the data controller is the University Data Protection Officer (10 Peas Hill, Cambridge CB2 3PN, tel. 01223 339888, fax 01223 331200 E-mail: data.protection@admin.cam.uk).

Your rights under the Act

You are entitled to have access to information held about you, except where releasing information would breach another person's privacy. You also have rights including rights to prevent processing likely to cause damage or distress and to prevent processing for the purposes of direct marketing.

How the Act will be Implemented at Cambridge University

l. The new rights and provisions will apply at different times depending on the kind of data involved, but for most information held by the University new provisions of the 1998 Act will apply from 23 October 2001. Until then, staff may continue to request access to their computerised data as they could under previous data protection legislation.

2. Under a long-standing agreement with the unions recognised for bargaining purposes, members of the Assistant Staff are currently able to access certain papers from their personal files held in the Assistant Staff Section of the Personnel Division (but see Procedure below).

Use of Personal Data

The Personnel Division holds and processes data and other relevant information for the purposes of personnel administration, record keeping, reference, monitoring and statistical reporting.

Responsibilities

1. The Personnel Division ensures that

    - All data retained within the Division complies with the principles of the Data Protection Act 1998.

    - All members of the Personnel Division are instructed not to process any data in a way that causes substantial unwarranted damage or distress to staff..

    - Staff data retained within the Division is processed only for the purposes for which it is held and, in particular, it is not processed for direct marketing purposes.

    - Staff data retained within the Division is not used for automated decision making without the consent of the individual member of staff concerned.

    - Staff files are kept securely and confidentially and made available to authorised persons only (see Appendix A). Heads of Institutions keeping information concerning staff ensure that it complies with the Act. It is expected that such information would normally be the same as that held in the Personnel Division.

2. Heads of Institutions retaining any information concerning staff must ensure that it complies with the Act. Ideally, such information should also be lodged with the Personnel Division.

3. Individual members of staff are responsible for informing the Personnel Division of any changes in their circumstances which might affect the accuracy of data held, which should preferably be notified at the time of the change or at the time of any check conducted by the Personnel Division.

Data on Individuals

1 Members of the Personnel Division will ensure that information held by the Division for personnel management purposes complies with the requirements set out in Appendix B.

2 Departmental Managers who hold staff records are required to ensure compliance with Appendix B.

3 Staff have certain rights of access to electronic records and, save for the exception relating to members of the Assistant Staff, as described above (giving them a continuing right of access to paper records), from 23 October, 200l, to certain paper records kept on them within the Personnel Division or elsewhere. All requests, including those from members of the Assistant Staff, for access to this information should be made to the University Data Protection Officer.

Data may be withheld where it would disclose personal information about another data subject.

4 Under the Act, the University is not required to disclose the references it provides in respect of staff applying for other employment. These references may be disclosed by organisations receiving them. References should therefore always be written on the assumption that they may be seen by the subject but, when providing references, University staff should include a statement as to whether or not they agree to disclosure. One way of avoiding such problems might be to send a copy of the reference to the data subject at the time it is written.

5 Written references for job applicants will be sought in confidence and applicants and referees will be advised of this practice. Referees should also be requested to indicate in writing whether or not they would agree to disclosure, if the data subject so requests. There is however no absolute guarantee that, even if the referees indicate that they would not permit disclosures to data subjects, that a data subject would not be entitled to require disclosure under certain legal requirements relating to, for example, defamatory comments or malicious falsehoods.

6 References provided by the University in respect of current staff applying for posts in other University Departments should be written on the assumption that they may be disclosed if a data subject so requests. Such references will be considered in the same way as any incoming reference.

7 Copies of references provided for current or former staff should be passed to the Personnel Division for retention on the central personal file.

8 Personal files for former staff will be retained by the University for

- The minimum period required in the event that a former member of staff makes an application to an Employment Tribunal.

- A further period of 7 years for reference purposes. Information not required for reference purposes will be removed from the file.

9 When staff leave the University, Heads of Institutions may retain files for a period, for ease of access when writing references. Heads of Institutions should then forward files to the Personnel Division. These files may continue be accessed, when necessary, upon request to the Personnel Division.

10 [A policy statement should be included here to cover the case where a University employee transfers from one department to another. This must ensure that the staff member is treated fairly, and that unfair/irrelevant material is not passed on to a new department.]

11 The University will retain for the minimum period applications, references and, as appropriate, interview notes in respect of candidates not appointed to the posts for which they apply. This is to ensure that information is available should a candidate complain of discriminatory treatment.

12 Staff seeking rectification and/or destruction of personal data should apply in writing to the University Data Protection Officer, clearly stating their reasons.

Further information and advice on data held on individual staff for personnel management purposes may be obtained from the Personnel Division.

Annex 8 - Data transfer between Colleges and the University

[authors Dr P B Wilson and Dr G Reid]

1. Mechanism:

Offer letters will include copy of declaration to be signed on admission, with text in letter either, e.g. "This offer is made conditional on the acceptance, for the benefit of the College and the University, of the terms of the Matriculation Declaration, that acceptance to become irrevocable on admission to membership of the College", or, e.g. " I enclose a copy of the declaration that you will have to make on matriculation".

October: Students sign declaration on matriculation, and are provided with information in *The Student Handbook* on nature of data to be processed.

2. Draft declaration:

[Matriculation statement]

I understand that in becoming a member of [College] I accept the responsibility of membership of the College and University community, and agree to abide by the statutes, rules and regulations of these institutions and to do nothing that is harmful to the work or reputation of either of them.

I consent to the processing by the College and the University of personal data (including sensitive personal data, as defined in the Data Protection Act 1998) about me for the proper purposes of those institutions.

I undertake to observe the provisions of the Data Protection Act 1998 in relation to any personal data I may myself hold and process as a student of the College and the University, and I agree to indemnify the College and the University from liability for any claims or damages that may arise from the processing of this data.

3. List of points for *Handbook* paragraphs

Data to be processed will include the following (this is digested from the *Student Data Model Specification*: the paragraphs in the *Handbook* will not necessarily be in list form).

Personal data

Non-academic

identification (name, gender, date of birth, photograph)
location (home address, term-time address, emergency contact address, temporary address; telephone numbers; e-mail address; web home-page URL; College affiliation; country of ordinary residence
social (marital status, children, ethnicity, disability, social class, nationality, religion, dietary requirements, parental occupation, electoral roll, bank account, GP, matriculation details). Note that much of this is sensitive data, required for statistical purposes: access control will need to be strict.
career (employment where appropriate; hobbies/ interests/ achievements

Academic

school history including examination results
higher education history

Current student data:

A. Programme and course data

progress data re residence/ degrading etc., inc. any Application Committee references
feedback from student (self-assessment, teaching assessment)
examination entry and record including marks for individual papers as well as overall classicification
Faculty/Department data (advisors, course assessments etc.)

B. College data

College Advisors: Tutor, Director of Studies
Residence record
College Supervisions: record of supervisors and supervisions given; supervisors' reports (restricted access)

C. Financial data

Fee status, source of fees, supporting bodies, record of fee payments

Note: Colleges clearly hold a range of material not directly covered here: admissions files of current students, references, correspondence relating to examinations, finances, health, non-academic achievements, disciplinary matters etc. Tutors and Directors of Studies will hold data in their own personal filing systems.

Among other points for inclusion in the *Handbook* text will presumably be the following:

- information about licence holders and data controllers
- information about the forms in which data will be processed and reference to College and University information security policies
- information about publication of relevant data, e.g. over internet, posting of examination results

Annex 9 - Draft JISC Code of Practice on Examinations

[author Andrew Charlesworth]

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 Examiners' comments

External examiners' 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 internal 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 identity numbers instead of names;
- providing results directly to each student face-to-face, via post, or via secure electronic means.

Annex 10 - Draft JISC Code of Practice on Security of data

[author Andrew Charlesworth]

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, as a minimum, ensure that:

- wherever possible, data are de-personalized, or coded, or encrypted, with any key being kept securely.

- Existing and proposed personal data processing operations are evaluated to ascertain and evaluate all 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 life, 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 culture 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) will be a disciplinary offence

- 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), 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. Institutional regulations should 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 found in areas where personal data is held or processed without proper credentials.

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.

- 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

Employee and student use of personal data on home computers or at remote sites.

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 have an up-to-date virus scanning program installed on laptop computers or personal machines and scan all disks for viruses prior to loading.

- they back up system hard drives to avoid loss of data.

- they report all computer security incidents including virus infections to the institution

- when using laptops they:
  - keep the laptop constantly in view when travelling, especially in airports;
  - store the laptop in the boot of an vehicle in which it is left unattended
  - 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

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.

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 are discarded

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 [what] 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, HE and FE 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

Annex 11 - Draft JISC Code of Practice on The Internet and World Wide Web

[author Andrew Charlesworth]

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. Within the set of webpages that make up an institutional website there will be webpages that contain personal data. The personal data in question is usually in the form of text and pictures, and primarily relates to the role that certain individuals play in the institution. That data is, by virtue of the background technology, available both outside the institution and outside the UK, including countries outside the European Economic Area (EEA) that do not have data privacy regimes considered adequate by the EU Commission.

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 the 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 website, including the use of photographs of data subjects for general publicity (background shots, panoramas etc.) where the data subject is clearly identifiable will require the consent of the relevant data subjects. Where such consent is not forthcoming, the personal data in question should not be used.

- HE and FE institutions may use non-sensitive staff personal data on institutional 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

- HE and FE institutions should obtain the consent of all data subjects, staff and student, to use non-sensitive personal data (including photographs) on institutional webpages, 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 webpages without explicit consent.

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 internal use. 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 outside the institution 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.

- HE and FE institutions may use internal institutional staff and student on-line telephone and e-mail directories 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 external staff on-line telephone and e-mail directories 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 outside the institution 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
  - the period for which the data will be kept

- 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.

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:

- 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 of their data 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

Annex 12 - Draft JISC Code of Practice on CCTV

[author Andrew Charlesworth]

CCTV and similar surveillance equipment

HE and FE institutions are increasingly using CCTV systems across their sites to ensure site security and the safety of staff, students and visitors. As users of CCTV and similar surveillance systems they will need to comply with the provisions of the 1998 Act. 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 and similar surveillance equipment 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 and similar surveillance equipment.

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.

Annex 13 - Alumni Databases and the new Data Protection Act

Summary of a meeting held between UK University representatives of CASE (the Council for Advancement and Support of Education) and the Data Protection Registrar's Office (now ODPC). (Wilmslow 25 January 2000)

Any comments or recommendations made below are based on the informed opinions and advice passed on to us by staff at the ODPC.

Data Controllers in charge of Alumni Databases will clearly need to develop a broad working knowledge of the Act, as each potential new use of data that comes along will need to be considered in the light of four factors: the Act itself; the notification under which alumni data is registered; the level of consent received and required for the relevant processing, and the latest guidance received from the ODPC.

It is envisaged that a further meeting will take place, perhaps in late 2000/early 2001, to ensure that the guidelines below remain up-to-date.

1. Notification of Purposes.

Standardisation for Universities

The ODPC is working towards a 'standard' notification ('registration' under the previous Act) for all Universities, which could be amended by individual institutions for any additional needs, but which would be likely to cover their day to day data processing needs. A draft version has recently been sent to Universities for comment.

It was suggested, and in principle agreed, that it would be helpful to add 'Alumni Relations and Development' as a separate heading within this document, in order to ensure that any such template would cover the needs of Alumni and Development offices consistently and in one section, which could then be up-dated for all universities at the same time, as and when necessary.

Need for separate Notification for certain affiliated bodies

If a body associated with the University (e.g. University Trust) constitutes a separate legal entity, a separate notification should be registered with the ODPC.

2. Processing where positive consent is not required.

The ODPC agrees that alumni might 'reasonably expect' Alumni Offices to process their data for the following purposes, which do not therefore require explicit 'positive' consent.

- Sending University mailings (e.g. Alumni magazines, Newsletters, Annual Reports)
- Sending University mailings to offer benefits, services and affinity products to alumni (although see 5. Below)
- University-related fund-raising initiatives (although see 7. below)
- Seeking non-financial alumni support (e.g. careers advice to students, help with student recruitment)
- Contacting alumni regarding events and reunions which are relevant to them
- Use of Mailing Houses for large-scale mailings (with confidentiality agreements in place)
- Forwarding of messages from other graduates (without disclosing data)
- Including information on products and services which may be of interest to alumni within University mailings (e.g. Affinity Card materials)

Although explicit positive consent is not required for these purposes, the ODPC advises that Alumni data controllers need to let alumni know that they have certain rights relating to the data held on them, and that they have the right to object to use of their data for direct marketing purposes. As long as these rights were communicated, consent for the above purposes could be considered to be on-going. Best practice would also see the inclusion of 'opt out' statements when we use their data for a particular purpose.

For example, if we forward a message on behalf of another graduate, the ODPC advises that we should enclose with that message a standard statement, explaining that we have forwarded the message without disclosing the address, but that if they would prefer us not to forward similar messages in future, they have the right to request this.

We do not, therefore, need to include several tick boxes on questionnaires to allow individuals to opt 'in' or 'out' of each of the specific purposes listed above. Questionnaires should, however, include a reasonably detailed statement about the purposes for which data is processed (see Appendix A for a suggested statement, although each institution will clearly wish to tailor this to match their own data processing needs).

Data controllers will also need to ensure that databases can flag up those individuals who request that their data is not used for a particular purpose, and will need to ensure that this data is cross-referenced before future communications relating to a particular purpose are processed.

To summarize on this point, the ODPC advises that the first question it is likely to ask of an institution (following a complaint from one of their data subjects) is "what opportunity was the individual given to object to the use of their data for that purpose, and, if any objection was made, was it acted upon?"

3. Sharing of data with branches of Alumni Associations, and other recognised affiliated bodies, individuals, organisations or agents, for University/Alumni Association purposes.

Examples of groups/organisations/individuals which might be involved:

World-wide branches run by volunteers under the umbrella of the University Alumni Association.*
'American Friends of the University of XX'*
In-country University employees with in-country responsibility for alumni relations*
Other less formal groups of alumni and alumni contacts*
British Council Offices for the purposes of publicising joint alumni events*
Publishing Companies acting on behalf of the University in preparing an Alumni Directory*

** See also 8. Below on Transfer of Data outside of the EU.*

The ODPC is reasonably comfortable with sharing of data with such groups for alumni purposes, on four conditions:

1. That Data Protection statements circulated to alumni (such as on questionnaires and mailing cover sheets) make mention of this generic type of purposes (see suggested statement on Appendix A)

2. That alumni are given the opportunity to object to the disclosure of their data for this type of purpose.

3. That confidentiality agreements are in place, whereby those receiving data guarantee not to disclose it to third parties.

4. That where an agent (e.g. publishing company) is involved, a contract is in place that stipulates that the company is acting as a Data Processor for the University, and that where the company makes direct contact with alumni, any materials sent out make it clear that they are acting as an agent of the University.

4. 'Host' mailings for outside companies.

'Host' mailings are those undertaken by an organisation on behalf of an outside company, where no data is shared. For example, Universities are occasionally approached by outside organisations (such as recruitment consultants) to send a mailing to a particular set of alumni, sometimes in exchange for a fee. There is a distinction here between this type of mailing and including 'inserts' in a University-related mailing (e.g. of an Alumni Magazine), a purpose which is included under 2. above. Where a 'host' mailing is concerned, the purpose (and target audience) of the mailing is driven by the wishes of the Company, without whose involvement the mailing would not take place.

The DP Office considers 'host' mailings to be 'trading in personal information' and advises that it should not be undertaken without the prior positive consent of individuals (see 6. Below). The mailing could therefore only go ahead for those alumni providing such consent. It would also be best practice to include a further 'opt out' clause within each resulting mailing, in case individuals wish to object at a later stage.

Since the meeting, Phil Boyd (Senior compliance Manager at the ODPC, who was present at the meeting) has advised that:

"the position of universities differs significantly from that of other organisations which may be offering host mailing facilities. This is to do with the circumstances under which the University obtains the personal data of its alumni and the period of time that is almost certain to elapse between first obtaining these details and subsequently offering a host mailing facility."

5. Sharing of Data with Banks and other commercial partners for Affinity products and services

The ODPC does not consider that alumni might 'reasonably expect' Alumni Offices to share their data with Banks and other affinity partners for the purposes of marketing Affinity Credit Cards or other products or services, and advises that we should not share any data in this way without the prior positive consent of individual data subjects (see 6. below).

The ODPC staff advise that they have received a number of complaints from alumni data subjects on this particular issue.

Inserting information from affinity partners inside University mailings (without disclosure of data) has been included under section 2. above, where positive consent is not required. Similarly, mailings sent by a University to its alumni specifically to offer affinity services (but without disclosure of data to affinity partners) are covered under section 2.

6. Interpretation of 'positive consent' as and when it is needed for alumni processing.

The optimum form of positive consent is to have a signed copy of a Data Protection or other Statement where the individual has positively opted 'in' to the type of processing mentioned.

However, where alumni databases are concerned the ODPC is happy to include within its definition of positive consent an individual *not* ticking an 'opt out' box on a form, where mention is made of a purpose, ***but only under circumstances where the form itself must be returned***.

In seeking further clarification, three specific scenarios were discussed :

Scenario 1: Where a student has to sign and return a form in order to receive their degree.

Assuming the relevant purpose was included in a data protection statement on that form with a separate 'opt out' box, and the individual does not tick the box, then the DP Office would consider this adequate consent.

Scenario 2: Where an individual alumna/us returns a questionnaire

If a similar 'opt out' box is included as part of a data protection statement on an alumni questionnaire, and an individual returns that questionnaire without ticking the box, that would also be interpreted as adequate positive consent for that purpose.

Scenario 3: Where an individual alumna/us does not return a questionnaire

If a similar 'opt out' box is included as part of a data protection statement on an alumni questionnaire, those who do *not* return the questionnaire cannot be considered to have offered adequate consent for any of the particular purposes listed which require positive consent.

7. Processing of Sensitive Data

It was felt by those present that alumni databases were unlikely to be processing sensitive data (as defined in the Act) on a regular basis. Storing of information such as ethnic origin for monitoring purposes is acceptable, but must not be processed for any other purposes without the explicit consent of the data subject.

8. Telephone Preference Service

The ODPC's current interpretation of an 'unsolicited' telephone call to any individual signed up to the Telephone Preference Service (TPS) is a call that has not been specifically requested, irrespective of the nature of any on-going relationship between the individual and the organisation.

The ODPC agreed to look further into the definition of 'unsolicited', and how it applies to alumni databases and telephone-based fund-raising programmes. Clarification was sought, for example, on where a University stands if an individual who is signed up to TPS returns a questionnaire to which they have added their telephone number, and signs a data protection statement which mentions fund-raising and the possible use of data provided for direct marketing purposes.

Since the meeting, Phil Boyd has passed on the following advice:

"So far as the TPS is concerned, it seems to me that the position is that fund-raising approaches by telephone should not be made to any alumni who have registered with the TPS unless they have indicated that they are happy to receive calls from the University. While in some cases it may be difficult to judge whether the call has been invited, it would seem to me that if an alumna/us has provided a telephone number on a questionnaire which itself clearly refers to fund-raising and marketing activities then it would be reasonable to make use of that telephone number. We would

certainly be content for you to proceed on that basis providing that there was a general commitment to review the position in the event of any complaints."

9. Transfer of Data outside of the European Economic Area.

The ODPC is waiting for some sort of consensus to emerge out of meetings of EU Data Protection Commissioners and also wishes to take further legal stock of the situation. In the meantime the ODPC were able to confirm that data could be transferred outside of the European Economic Area if the specific consent of the data subject had been obtained.

It was confirmed that any data posted on the Internet should be considered as data transferred outside of the European Economic Area. However, the ODPC would only be concerned if data were published about an individual that was either sensitive, or which provided a means of contacting that individual without his or her prior positive consent. Publishing of 'lost' alumni lists on the Internet, where information was limited to name, department and year of graduation, for example, would not worry the ODPC.

10. Maintaining a 'skeleton' record when removing an individual from the Database.

The ODPC advises that the Act recognises that where an individual requests to be removed from the database, data controllers need to be able to maintain a 'skeleton' record, flagged up to make sure that further contact is not made, to safeguard against re-entering that individual from a separate data source in the future.

11. Checking validity of addresses

The ODPC encourages Alumni data controllers, where possible, to check addresses against the electoral roll, particularly where no response has been received from a particular address for several years. The ODPC does, however, appreciate that Universities will need to use their own discretion here, as in some circumstances mail may be reaching an individual even though the officially registered surname at that address does not match the surname on the institution's database.

(continued…)

Appendix A

Suggested Data Protection Statement for Alumni Questionnaires

1998 Data Protection Act

All data is securely held in the University Alumni/Development Office and will be treated confidentially and with sensitivity for the benefit of the University of X and its members. The data is available to our international offices, colleges, faculties, academic and administrative departments, recognised alumni societies, sports and other clubs associated with the University, and to agents contracted by the University for particular alumni-related projects.

Data is used for a full range of alumni activities, including the sending of University publications, the promotion of benefits and services available to alumni, notification of alumni events and of programmes involving academic and administrative departments. Data may also be used in fund raising programmes which might include an element of direct marketing.

Under the terms of the 1998 Data Protection Act you have the right to object to the use of your data for any of the above purposes.

Annex 14 - Draft JISC Code of Practice on Employee use of personal data

[author Andrew Charlesworth]

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 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 a regular 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 within HE and FE institutions

Employees will often be expected to collect, hold, and process significant amounts of 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.

- FE and HE 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.

- FE and HE 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

Annex 15 - Draft JISC Code of Practice on Student use of personal data

[author Andrew Charlesworth]

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 within FE and HE institutions

Students may on occasion be in a position to access personal data held and processed within FE and HE 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.

- FE and HE 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

- FE and HE 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.

Annex 16 - Draft JISC Code of Practice on Data on Disability Service Provision

[author Andrew Charlesworth]

A key area where HE and FE institutions will need to collect and process sensitive data is that of service provision for disabled staff 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.), but collection of disability data may also occur throughout the period of study. The use of 'blanket' consent forms is inappropriate for many forms of data collection, but particularly so for collection of sensitive personal data, including disability data.

- 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 students against discrimination, harassment, and victimisation that may arise from any disclosure of their disability status.
- clear and readily accessible remedies for disabled 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. (potential employers)
- 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;
- procedures that both protect an individual's privacy and permit necessary disclosure for the provision of effective support for disabled students or to ensure health and safety.