

Data Protection

- 1. Introduction..... 1
- 2. Freedom of Information and Data Protection 1
- 3. 'Personal Data' and the Durant case..... 2
- 4. 'Personal Data' and the FOIA 2000..... 3
- 5. Obligations on those processing of Data 5
- 6. FE and HE Institutional Compliance..... 6
- 7. Conclusion..... 8
- 8. Some Key Definitions..... 9

Author - Andrew Charlesworth

1. Introduction

By April 2005, the Data Protection Act 1998 (DPA 1998) will have been in force for five years. During this time the Act has had a significant effect upon the ways in which FE and HE institutions handle their personal data processing.

Today, across FE and HE institutions, all computerised processing of personal data, many structured manual records, and even some unstructured manual records are subject to provisions of the DPA 1998, including the right of the individual to access the data which is held about them. Together with the Freedom of Information Act 2000 (FOIA 2000), the DPA 1998 has forced a re-think of institutional good practice in personal data handling, required new approaches to records management and made institutions consider more carefully their obligations to those whose data they hold.

Data protection law has not been static during this time – various aspects of the DPA 1998 have been subject to judicial interpretation, and the FOIA 2000 has made amendments to the DPA 1998 with particular reference to 'public authorities', the definition of which includes both FE and HE institutions.

Data Protection Act 1998 – Factsheet

- Was passed in 1998 and came fully into force in 2001
- Was amended by the FOIA 2000 to cover additional issues in relation to public authorities, including colleges and universities
- Covers all personal data processed by FE and HE institutions, including computerised data, structured manual files and unstructured data, except where specifically exempted.

The DPA gives individuals certain rights regarding information held about them. It places obligations on

those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual. Anyone processing personal information must notify the Information Commissioner's Office (TICO) (<http://www.informationcommissioner.gov.uk/>) that they are doing so, unless their processing is exempt. Notification costs £35 / year.

The Eight Principles of Good Practice

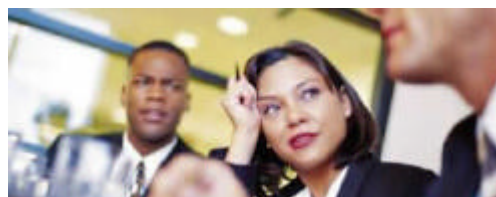
Anyone processing personal information must comply with eight enforceable principles of good information handling practice. These say that data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the individual's rights
7. secure
8. not transferred to countries outside European Economic area unless country has adequate protection for the individual

2. Freedom of Information and Data Protection

TICO oversees both the Freedom of Information Act 2000 and the Data Protection Act 1998. Both Acts affect information policy and practice. They overlap where personal information is considered for disclosure. Joint responsibility allows the Information Commissioner to provide a single point of contact for public authorities and the public.

The FOIA 2000 extends the rights of the individual to access their data which had already existed under the DPA 1998. The definition of 'data' is widened, as far as public authorities are concerned, to include all other 'recorded information held by a public authority'. However, there are limits to the data subject rights that apply to this additional category of data (see below).



A request by an individual for information about him or herself is exempt under the FOIA 2000 and should be handled as a 'subject access request' under the DPA 1998. In certain circumstances, such a request may involve the release of associated information in which case the provisions of sections 7(4) and (5) of the DPA 1998 should be used to determine whether it is appropriate to release the third party information.

Where an applicant specifically requests information about a third party, or where responding to a request for information would involve the disclosure of personal information about a third party (which is not also personal information about the applicant), the request falls within the remit of the FOIA 2000. However, the authority must apply the Data Protection Principles when considering the disclosure of information relating to living individuals. An authority must not release third party information if to do so would mean breaching one of the Principles.

Where the disclosure would not breach the principles, the authority may release the information. However, if the third party has served notice under s.10 DPA 1998 that disclosure would cause them unwarranted substantial damage or distress, or the third party would not have a right to know about the information relating to them or a right of access to it under the DPA 1998, the institution is required to consider whether release of the information would be in the public interest.

3. 'Personal Data', 'Relevant Filing Systems' and the Durant case

The DPA 1998 defines personal data as any information that relates to an identified or identifiable person (the data subject), or which in combination with other information in the possession of, or that is likely to come into the possession of, the data controller would permit their identification.

The Durant Test

This definition of 'personal data' was considered by the UK Court of Appeal in the case of *Durant v Financial Services Authority* (2003). In *Durant* the Court of Appeal did not consider the issue of the "identifiability" of an individual, but concentrated on the meaning of "relate to". The Court decided that data will relate to an individual if it: "is information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity". The Court identified two issues that may aid in determining whether information "is information that affects [an individual's] privacy" and, thus, "relates to" an individual:

"...whether the information is biographical in a significant sense that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations..."

"The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest ..."

If an individual's name appears in information, the use of the name implicates 'personal data' only where its inclusion affects the named individual's privacy. Thus, the fact that an individual's name appears on a document, does not mean the information contained in that document will necessarily be personal data about the named individual. It is more likely that an individual's name will be 'personal data' where the name appears together with other information about the named individual such as address, telephone number or information regarding his hobbies.

TICO suggests that the following examples of information will not normally be personal data:

- mere reference to a person's name where it is not associated with any other personal information;
- incidental mention in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity;
- where an individual's name appears on a document or e-mail indicating only that it has been sent or copied to that particular individual - and there is no other information about the individual within it.

The Court of Appeal also considered the definition of 'relevant filing system' and held that it was to be more narrowly construed than had been previously advised by TICO.

A 'relevant filing system' is a "system":

- in which files are structured or referenced so as to clearly indicate at the outset of the search whether specific information capable of amounting to personal data of an individual making a subject access request is held within the system and, if so, in which file or files it is held; and
- which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located.

TICO has now suggested using what it calls the "temp test" to assess manual filing systems. In other words, if an institution employed a reasonably competent temporary administrative assistant, would they be able to extract specific information about an

individual without any particular knowledge of the work that the institution does or the documents that it holds, after only a short induction, explanation and/or operating manual on the particular filing system. If a temp could locate the information easily, the information will be held in a relevant filing system. TICO's guidance notes that very few manual files are currently likely to be caught by the DPA 1998 under this definition.

Institutions should be aware that the interpretation of these definitions may change either in subsequent case law or by a change in the law and should check TICO's website for updates.

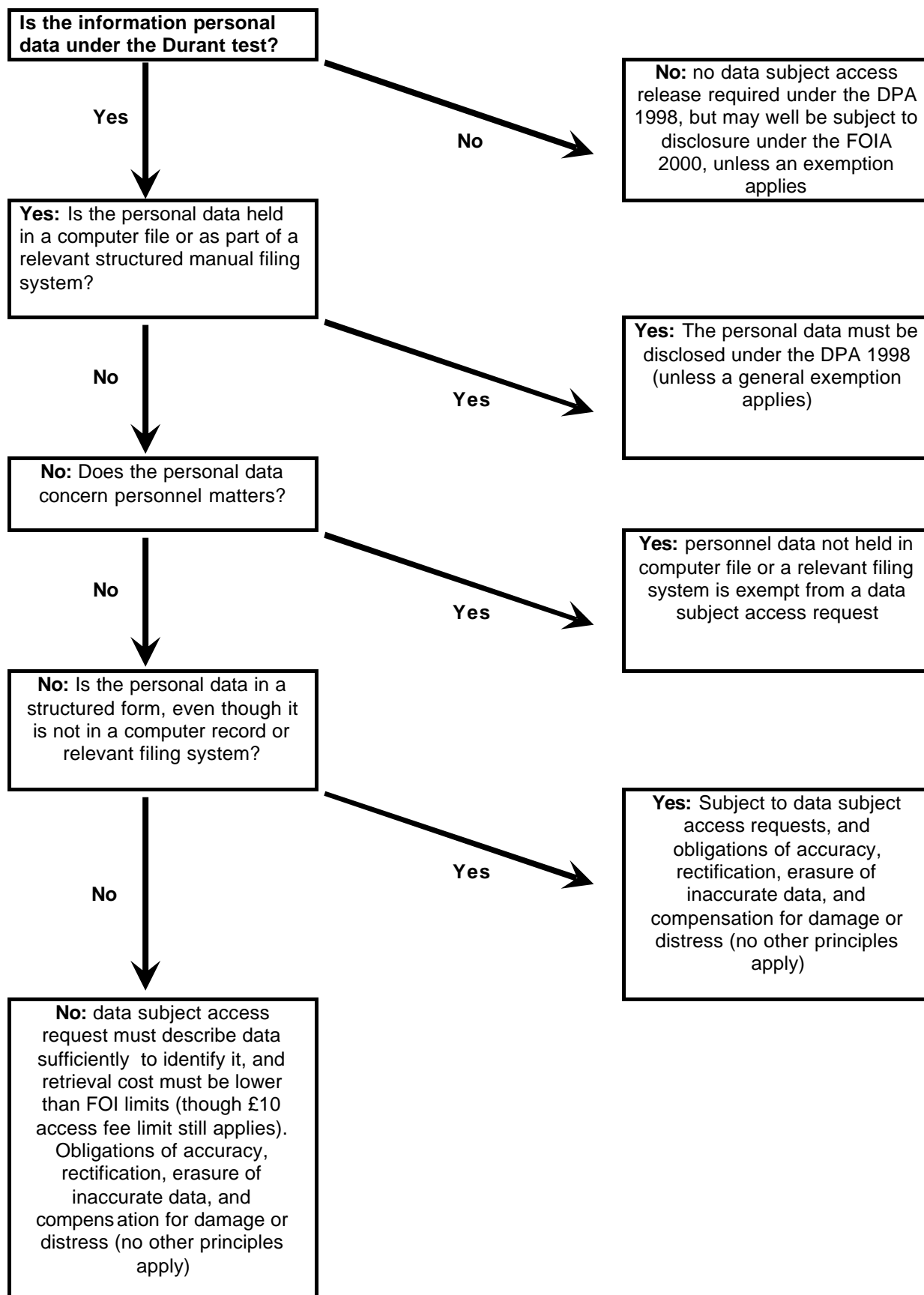
4. 'Personal Data', 'Relevant Filing Systems' and the FOIA 2000

The FOIA 2000 amends the DPA 1998 as to the scope of personal data which must be released under a data subject access request. The flowchart below is suggested for determining whether information held by a college or university (or other public authority) as a data controller is to be released. However, it should be remembered that the general exemptions to a data subject access request will always be available to the institution.

Exemptions to Data Subject Access Requests

- Request not in writing
- Required fee not received
- Requester not able to verify identity upon request
- Disclosure would require disclosure of third party's personal data, and third party has not consented where it would be reasonable to require consent
- Disclosure would require disclosure of third party as source of personal data, and third party has not consented where it would be reasonable to require consent
- Exemptions in secondary legislation (e.g. regarding certain health records, school educational records, social work records)

Data Subject Access - Flowchart



5. Obligations on those who control the processing of Data

Processing

Schedule 2 DPA 1998 lists specific conditions for all processing of personal data and Schedule 3 DPA 1998 lists specific conditions for the processing of "sensitive" personal data.

The six conditions

For "ordinary" personal data, at least one of the following conditions must be met for personal information to be considered fairly processed: The conditions are:

- the individual has consented to the processing
- processing is necessary for the performance of a contract with the individual
- processing is required under a legal obligation (other than a contractual one)
- processing is necessary to protect the vital interests of the individual
- processing is necessary to carry out public functions, e.g. administration of justice
- processing is necessary in order to pursue the legitimate interests of the data controller or third parties and is not unfair to the individual

For "sensitive" personal data, one of the ordinary processing conditions and one of the conditions for processing sensitive data must be met before processing can be carried out. The conditions for processing sensitive data are that the data subject has given his or her explicit consent to the processing of the personal data, or that the processing is necessary for a further set of specified reasons, including:

- It is required by law for employment purposes
- It is needed in order to protect the vital interests of the individual or another person
- It is needed in connection with the administration of justice or legal proceedings

The precise meanings of "consent" and "explicit consent" remain undefined, although the latter is increasingly regarded as meaning "in writing". If no consent is forthcoming and the purpose of particular processing is not otherwise on the list of permissible reasons, it will be illegal.

Data subject rights

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

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

Failure to respect these rights may lead to civil or criminal action against the data controller as an institution and, in circumstances where senior management are considered to have consented to, colluded in, or been negligent over, breaches of the Act, they may be individually prosecuted.

Exemptions

The Act provides wide exemptions for journalistic, artistic, or literary purposes that would otherwise be in breach of the law. These exemptions apply if the processing is with a view to publication and the data controller reasonably believes both that publication would be in the public interest and that to comply with the relevant data protection provisions would be incompatible with the special purposes. The journalistic exemption was raised as a defence in the cases of *Campbell v. MGN*, and *Douglas v Hello*, but while the Douglas's won nominal damages under the DPA 1998, neither case added much to general understandings about the Act, either in terms of exemptions, or in terms of what constitutes 'significant damage or distress'. It is in any case unlikely that academic research and publishing will normally have recourse to this set of exemptions, and while there is a wide range of other exemptions, most of those are inapplicable to the activities of FE/HE institutions on a general basis but may be used in specific cases, for example if disclosure without consent is required to the police or for legal proceedings.

Disclosure to Third Parties

The DPA 1998 permits the disclosure of an individual's personal data by an institution, even without their consent, where that disclosure is carried out in accordance with the Schedule 2 and 3

conditions for processing, and where the data subject has been informed that such disclosure may occur. The DPA 1998 itself does not oblige institutions to disclose personal data to specific third parties, but s.35.(1) states that personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

Certain third parties may therefore require disclosure of an individual's personal data by an

institution. Institutions should however, where possible, ensure that students are properly warned of any known statutory disclosures that they are required to make. The Act makes no explicit reference to the nature of data that may be demanded by statutory obligation, so institutions should be able to disclose to any properly grounded statutory request without falling foul of the law. A non-exhaustive list of third parties who may require disclosure by an institution are included in the following table.

Table 1 – Examples of Disclosure under DPA

Third Party	Authorisation for disclosure
UK Funding Councils e.g. HEFCE HEFCW, and their agents e.g. QAA, HESA, HEFCE, SHEFCE auditors.	Further and Higher Education Act, 1992 s.79 - Duty to give information to the funding councils.
Electoral registration officers (voter registration)	Representation of the People Act 2000; The Representation of the People (England and Wales) Regulations 2001
Officers of the Department of Works and Pensions, and Local Authorities (benefit fraud)	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive (injuries and dangerous occurrences)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 s.3 - Notification and reporting of injuries and dangerous occurrences
Audit Commission and related auditing bodies (various)	Audit Commission Act 1998 s.6 - Auditors' right to documents and information.
Environmental Health Officers (notifiable diseases)	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Child Support Agency	Child Support (Information, Evidence and Disclosure) Regulations 1992.
Police Officers	Court Order - N.B disclosures to the Police are not compulsory except in cases where the institution is served with a court order requiring information.
Other third parties	Court Order - e.g. third party disclosure order.

6. FE and HE Institutional Compliance

Compliance with the DPA 1998 requires FE/HE institutions to consider the implications of many aspects of their operations, both in administration and in teaching. The compliance issues listed below are thus not exhaustive.

Holdings and processing data

The DPA 1998 covers all personal data processed by FE and HE institutions, including computerised data, structured manual files and unstructured manual data, except where specifically exempted.

It is thus important to:

- Review and ensure that the institutional notification is accurate, and that information provided to data subjects in collection notices is appropriate.
- Audit the accuracy and security of both computer files and manual filing systems, and,

where possible, work to reduce duplication of information within an institution to avoid inaccuracies and inconsistencies.

- Ensure that record management systems are suitable to support current institutional DP and FOI requirements, and that appropriate document lifecycle processes are properly adhered to and audited.
- Ensure that all staff receive DP and FOI training appropriate to their positions, and that refresher and update training is provided as necessary to guarantee continuing institutional compliance at all levels.
- Ensure that all communications from TICO, especially those relating to notification and compliance issues are passed on to, and dealt with expeditiously by, the appropriate institutional officeholder. Failure to respond to communications about non-compliance may lead both the institution and senior management being prosecuted.

New technologies, New opportunities

FE and HE institutions are constantly seeking to improve administrative processes, and the delivery of teaching. New technologies are constantly being developed and adopted to facilitate those objectives. In recent years, the use of "smart cards" as an integrated solution to issues such as building security, facilities usage, ID and campus payment systems has been a popular option. Currently there are a range of institutional and regional projects to develop lifelong learner record systems capable of transferring learner transcript information between academic institutions, and potentially to third parties, such as employers. All of these processes require careful planning to ensure that the personal data collections and transfers they may generate are handled in conformity with the DPA 1998.

When planning new systems it is important to:

- Identify the types of data collected, the purposes for which processed, and the appropriate Schedule 2 & 3 criteria to legitimise that processing
- Clarify the roles of those involved in the processing - data subjects, data controllers, data processors - and what their rights and obligations are
- Ensure that individuals are adequately informed why their personal data is being collected, the purpose it will be used for, and the types of party it may be transferred to
- Ensure that where necessary, consent or explicit consent can be obtained for proposed uses of personal data, and that should individuals withdraw consent for the processing of their personal data, as the Act permits, this can be achieved quickly and effectively.

Research data

The processing of any information relating to an identifiable living individual, including research, constitutes 'personal data processing' and is subject to the DPA 1998 including the eight Data Protection Principles. However, the DPA 1998 provides certain exemptions for "research purposes" including statistical or historical purposes. If the processing is not used to support measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, it is exempt from:

- The Second Principle, meaning that personal data can be processed for purposes other than for which they were originally obtained;
- The Fifth Principle, meaning that personal data can be held indefinitely;
- The data subject's right of access to his personal data, where the data is processed for

research purposes and the results do not identify data subjects.

In addition to the restrictive criteria in Schedule 3 of the DPA 1998 (explicit consent, medical research by a health professional, equal opportunities monitoring), the *Data Protection (Processing of Sensitive Personal Data) Order 2000* expressly permits processing of sensitive personal data for research purposes 'in the substantial public interest' where the sensitive personal data are not used to support measures or decisions targeted at particular individuals without their explicit consent; and no substantial damage or distress is caused, or is likely to be caused, to any person by the keeping of those data.

It is important to remember that:

- While some exemptions are granted for the use of personal data for research purposes, neither the DPA 1998 nor the *Data Protection (Processing of Sensitive Personal Data) Order* provides a blanket exemption from all the Data Protection Principles
- There should be an adequate institutional review process, in advance of use of personal data for research purposes, to ensure that the DPA 1998 can be adhered to; research should also be periodically monitored/audited for continuing compliance
- Requirements for appropriate security of data must be respected, including appropriate levels of security for sensitive data and security of data processed by researchers outside the institution
- Data may not be transferred to researchers in countries outside the EEA unless that country has adequate data protection regulations, or the explicit consent of data subject has been obtained, or there is an appropriate data protection contract with the recipient of the data
- Research data subjects should still be informed of any new purposes of data processing and the identity of the data controller and any disclosures that may be made.
- Research data subjects must be able meaningfully exercise their right to object to the data processing because it would cause/has caused, them significant damage or distress.

Marketing

Institutions wishing to use unsolicited electronic marketing communications for purposes such as alumni development and the solicitation of commercial/corporate sponsorship, must be aware of the new UK Privacy and Electronic Communications (EC Directive) Regulations 2003. These provide that:

- Unsolicited marketing calls should not be made to individual subscribers who have opted out either directly or by registering with the central stop-list, the Telephone Preference Service (TPS), or to corporate subscribers (e.g. companies) who have objected either directly or by registering on the Corporate TPS.
- Unsolicited marketing faxes should not be sent to individuals without their prior consent or to any subscriber who has objected, either directly or by registering on the Fax Preference Service (FPS).
- Unsolicited marketing emails or SMS should not be sent to any individual subscriber who has not consented unless the email address or phone number was collected in the context of a commercial relationship.

7. Conclusion

FE and HE institutions handle increasingly large amounts of student and employee personal information as well as study and research data which contains personal information. Getting proper data protection procedures and practices in place remains a crucial part of dealing with this often private and confidential information appropriately. A lack of clarity with regard to what can and cannot be done with personal data remains an obstacle to proper administration in many FE and HE institutions.

This paper attempts to add to the understanding necessary for compliance in addition to highlighting important concerns for FE and HE institutions.

7 April 2005

8. Some Key Definitions

Data Subject	The DPA 1998 defines a Data Subject as an individual who is the subject of personal data.
Personal Data	The DPA is only concerned with "personal data", that is, information relating to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Data concerning corporate bodies are excluded from the DPA, as are data concerning individuals who have died.
Consent	The DPA 1998 does not contain a definition of consent. If a Data Subject's consent is to be relied on to provide a Sch.2 criterion (Sch.2, s.1) for lawful processing, then the fact of consent cannot be simply assumed by a Data Controller (e.g. where a Data Controller sends out a form stating that in the absence of a negative response from a Data Subject their consent will be assumed). Where there is obvious inequality of bargaining power between the Data Controller and Data Subject, it may also be difficult to demonstrate the 'freely given' element of consent. Equally, consent may be withdrawn by the Data Subject at any point, a fact that may prove problematic for Data Controllers where consents are obtained for data processing purposes without which the Data Controller cannot provide an essential service. In such circumstances, reliance on another Sch.2 criterion, such as contract, would be more practical.
Data Controller	A Data Controller is "a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed". The fact that an individual or institution holds or processes personal data does not make them a Data Controller, if they do not determine the purpose and manner of that holding or processing.
Data Controller in Common	Data controllers who share personal data on Data Subjects for different purposes are referred to as 'Data Controllers in common'. Each Data Controller remains individually responsible for the processing they have carried out on the personal data.
Joint Data Controller	Data controllers who share personal data on Data Subjects for the same purpose, and who would be jointly liable for any breach under the DPA 1998, are referred to as 'Joint Data Controllers'.
Data Processor	A Data Processor is any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller. An employee of the Data Controller is regarded by the DPA 1998 as constituting part of the Data Controller. A Data Processor has no statutory obligations under the DPA 1998 as regards processing it carries out on behalf of the Data Controller. The DPA 1998 places the burden for ensuring that Data Processors do not allow breaches of the Act upon the Data Controllers who use them. Data Controllers thus need to ensure that their relationship with a Data Processor is governed by a formal Data Processing Agreement.
Data processing	Data processing is 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data.' This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. It is irrelevant whether these actions are manual or automated. The breadth of the DPA 1998 definition effectively means that from the moment of its collection, to the moment that it is destroyed or fully anonymised, personal data is being processed and must thus be treated in accordance with the Act.
Sensitive personal Data	Sensitive personal data are personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.

“...whilst I accept that time was taken up with the claimants' claim under the Data Protection Act [1998] which was successful only as to nominal damages, I must recognise, too, that the Act is of notorious obscurity...”
Lindsay J. in *Douglas v. Hello! Ltd* (No.7) (2004)

For a digest of IT Law relevant to FE and HE, subscribe to JISC-LEGAL-NEWS - see details at <http://www.jisclegal.ac.uk/newsletter.html>

INSIDE

This briefing paper examines:

- Recent data protection law developments in the *Durant v. FSA* case.
- The effect of the amendments to the DPA 1998 made by the FOIA 2000
- Areas of particular importance to FE and HE institutions

It is of interest to:

- DP and FOIA officers and their staff, in FE and HE institutions
- Senior Administrators and those responsible for developing future institutional records management and technology policy

This guidance should be read in conjunction with:

- Information Commissioner's Office, Factsheet: What is the Data Protection Act (DPA) <http://www.informationcommissioner.gov.uk>
- JISC Briefing Paper on The Freedom of Information Act 2000 accessible from the JISC Legal website at - <http://www.jisclegal.ac.uk/>

Author

JISC Legal wishes to thank **Andrew Charlesworth** of the Centre for IT & Law at the University of Bristol for writing this paper and **Louise Townsend** of *Pinsent Masons* for her comments.

7 April 2005