

15 August 2007

Please note: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

Table of Contents

1. Introduction	1
2. What is Data Protection?	2
3. Data Protection and FE and HE	2
4. Purpose of the Act	2
5. Application of the Act.....	2
6. Principles for Data Processing	3
7. Conditions for the Processing of Data	5
8. Rights of the Data Subject.....	6
9. Exemptions to Data Subject Requests	7
10. Enforcement	8

1. Introduction

This overview explains the application of the Data Protection Act 1998 (the 'Act') to UK further and higher education institutions (FE and HE institutions), with particular focus on the development and use of information and communication technologies. Institutions must be aware of the legal duties placed upon them when collecting or processing personal data. In technical terms, it is easy to devise a web form for users to input their details. Personal data may be collected and processed in a database or spreadsheet as part of a research project, and each institution is likely to hold substantial records digitally as part of its management information system. The digital world means that transfer of this data is potentially simple, and access from anywhere possible. For those wishing to perpetrate identity theft, such personal data may be very valuable, and leaking of data, at the best, is likely to impact a college or university's reputation.

As examples, in 2004, hackers gained access to up to 380,000 records at the University of California at San Diego, and in 2005, a laptop was stolen from the University of California at Berkeley, which contained unencrypted names, social security numbers and other details of around 98,000 course applicants. Although probably a petty theft, that information, if it had fallen into the wrong hands, may have permitted substantial identity fraud.

Institutions must ensure that, in their use of technology, personal data is protected appropriately. This confidence can be used positively, as a selling point, when it is achieved. Students, research subjects, and staff will all appreciate knowing that the institution takes their privacy seriously.

2. What is Data Protection?

Every individual has certain rights regarding the information that organisations hold, process or use about them. Data protection is all about ensuring that this information or 'data' is managed properly.

Data protection in the UK is governed by the Data Protection Act 1998. The Act came into force on 1 March 2000. It regulates the obtaining, holding, using, processing and disclosing of information relating to individuals. The Act applies both to manual data and data processed by computers.

The Act requires that those processing personal information notify the Information Commissioner's Office (ICO) (<http://www.ico.gov.uk>) that they are doing so, unless their processing is exempt. Notification costs £35 per year. It is illegal under the Act to process data without a notification, not in accordance with the notification and not to keep the notification updated.

3. Data Protection and FE and HE

The personal information of students, staff and members of the public are handled and processed by the FE and HE institutions for various purposes. The Act governs the way in which such institutions can use or process this information legally.

4. Purpose of the Act

The purpose of the Act is to protect the rights and privacy of individuals and to ensure that data about them is processed only with their knowledge and consent. For this, the Act gives individuals certain rights regarding personal information held about them and places certain obligations (in the form of eight principles) on those who process the personal information. Under section 1(1) of the Act, processing refers to anything that can be done with data. The people who determine the purpose and manner in which the information is to be processed are referred to as data controllers (e.g. any FE or HE institution) and those whose data are subject to process are known as data subjects (e.g. students, staff and alumni in an FE and HE).

5. Application of the Act

The Act applies to any personal data relating to any identifiable living individual. The Act thus does not cover information regarding deceased or anonymous individuals. It refers to two categories of personal data, namely that of 'personal data' and 'sensitive personal data'.

Under section 1(1) of the Act, personal data is any information about an identifiable living individual regardless of the format of the information. Though personal data must say something about an individual there are no prescribed conditions as to

where the data must exist for the Act to apply. The Act applies so long as it is the information about an identifiable individual. The Court of Appeal in *Durant v Financial Services Authority* considered the meaning of the term 'personal data'. It held that 'personal data' did not necessarily mean any and every document which has the data subjects name on it but the overriding test is whether the information in question affects a persons privacy, whether in his personal or family life, business or professional capacity. The information thus may be in the form of computerised personal data, on video tapes, CCTV footage or even data on paper files. It covers any data held in electronic formats (e.g. text files, emails, databases) and applies to manual data structured in a way where specific information regarding individuals is readily accessible. Some examples of such storage spaces in FE or HE institutions might be staff records, records in the library, careers service, individual departments or the accommodation office.

The Act also covers a category of personal data called 'sensitive personal data'. Section 2 of the Act refers to sensitive personal data to mean data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to 'personal data'.

6. Principles for Data Processing

At the core of the Act are eight data protection principles set out in Schedule 1 Part I. These constitute the obligations of an FE or HE institution towards their data subjects under the Act and data controllers processing personal information must comply with the eight enforceable principles. These provide that the data must be:

Principles for data processing	Explanation
1. fairly and lawfully processed	The data subject will have to be informed that their data is being collected, who holds their information, who the data controller is, what the data will be used for, an indication of how long the data will be kept and information on any disclosure to any third parties. One of the ways in which institutions can ensure fair and lawful processing of data is by issuing to its staff and students a data protection notice at the start of their employment or study. This notice should provide details regarding the purposes for which the collected data will be used.
2. processed for limited purposes	This principle requires that the data controller ought to know what he intends to do with the data he collects and he must not use data for purposes that it was not collected for. An FE or HE institution can thus under this

	<p>principle monitor the emails of its data subjects if the information discovered through monitoring is used only for the purpose for which the monitoring was carried out.</p>
<p>3. adequate, relevant and not excessive</p>	<p>This principle imposes an obligation on the data controller that the information collected must be adequate and relevant to fulfil the purpose for which it was collected. It must not be excessive in relation to the proposed use in question irrespective of whether the information is useful in the future. For example, collecting the email addresses of students in order to contact them regarding a lecture series will be considered as relevant and adequate. But collecting their dates of birth for this purpose will be considered excessive.</p>
<p>4. accurate and up-to-date</p>	<p>The purpose for which the data are used will be relevant in deciding whether updating of the data is necessary. This principle thus ensures that the data kept is accurate and up-to-date as holding data which is not accurate may not serve any purpose.</p>
<p>5. not kept longer than necessary</p>	<p>This principle simply obliges the data controller to keep the data only for the time for which the information is necessary to perform the operation for which it was collected.</p>
<p>6. processed in accordance with the individual's rights</p>	<p>The Act grants certain rights to the data subjects and this principle states that the data must be processed only in accordance with these rights.</p>
<p>7. secure</p>	<p>This principle requires that appropriate measures (technical and organisational) must be taken by data controllers against unauthorised or unlawful access to personal data and against accidental loss or destruction of personal data. It has significant application in an FE or HE e-learning environment. Since an e-learning system may include data such as student details, a student's submitted work and academic results; this principle makes it vital that such data are securely maintained.</p>

<p>8. not transferred to countries outside the European Economic area unless country has adequate protection for the individual</p>	<p>This principle limits the transfer of personal data to countries within the European Economic area (EEA). The transfer of personal data outside the EEA is not permitted unless the country has an adequate level of protection. So, FE and HE institutions in the UK should be mindful regarding the exchange of personal data in student or staff exchange programmes with a non-EEA institution.</p>
--	--

7. Conditions for the Processing of Data

The Act lists certain conditions under Schedule 2 of the Act for the processing of personal data and sensitive personal data. Personal information is considered to be fairly processed only if at least one these six conditions below are met.

1. the individual has consented to the processing: One of the conditions for the processing of any personal data is that the data subject has given his consent to the processing. If the data subject gives his consent but changes his mind later, any data published about him must be removed immediately. Care should therefore be taken by institutions before publishing without consent the email addresses or home addresses of students on a department notice board. This could be considered unfair processing of the individuals' data.

2. processing is necessary for the performance of a contract with the individual: An example of the application of this condition could relate to the disclosure of student data. Students undertaking research towards a higher degree at institutions could be funded by industry sponsors. In such arrangements, the student might be involved as a party to the contract with the outside sponsor. The disclosure of student data (which could be treated as processing of data) to the sponsor might be required for performance of the contract so that the sponsor is informed of the student's progress on his research.

3. processing is required under a legal obligation (other than a contractual one): Data could be considered as fairly processed where an institution legally obliged to disclose personal data discloses personal data of staff or student for statistical purposes like of ethnic or disability monitoring.

4. processing is necessary to protect the vital interests of the individual: A typical situation to illustrate this condition is where disclosing the staff or student personal data to a third-party is required to fulfil a medical emergency.

5. processing is necessary to carry out public functions, e.g., administration of justice.

6. 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 example, many FE and HE institutions operate CCTV systems within the institution. Under this right, FE or HE institutions using CCTV for anything other than the most basic of surveillance will have to comply with the DPA.

In order to process sensitive personal data, the Act requires that in addition to satisfying one of the ordinary processing conditions mentioned above, the data controller must also fulfil one of the extra conditions below: They are:

1. the data subject must have given his or her explicit consent to the processing of personal data: Counselling services offered at institutions present a good example where institutions might act as data controllers processing the sensitive personal data of their data subjects. Staff and students who experience emotional, psychological problems might approach the counselling service at their institution for advice and support. In such a situation, the counselling service might be required to record the data subject's sensitive personal data (their physical or mental state of health). The counselling service is required in these situations to obtain explicit consent, if possible in written format, prior to processing any sensitive personal data.

2. the data is required by law for employment purposes.

3. the data is needed in order to protect the vital interests of the individual or other person.

4. the data is needed to deal with the administration of justice or legal proceedings.

8. Rights of the Data Subject

The rights granted by the Act to data subjects are applicable to anyone, anywhere in the world if the institution holds their data. The individuals have seven rights in respect of the personal data held by them. These are:

- **The right to subject access:** This right allows a data subject to be informed of the information held about them and to discover to whom it has been disclosed. The request for access must be made in writing (including fax and email) and an institution must respond to the request within a period of 40 calendar days. Some examples of the application of this right is:
 - A data subject has the right of access to information that was held about them by a university which could include email correspondences, any particular items of correspondence and also information which might be considered sensitive personal data.
 - A data subject has the right of access to copies of job references received about them from another person or organisation by the FE or HE institution.

- **The right to prevent processing:** A data subject has the right to object to and prevent processing of information held about them if it is likely to cause substantial damage or distress to the data subject.
- **The right to prevent processing for direct marketing:** If personal data is processed for direct marketing process, the data subject can object and opt out of this. FE or HE institutions that hold data of their alumni may use it for marketing and publicity of the institution. In such cases, the alumni have the right to object to this and can request that their personal data is not processed for such purposes.
- **The right to prevent automated decision-taking:** This right allows a data subject to object to decisions about them being made only by automatic means. In situations where automated marking of examinations is done, a student has the right under the Act to object to such automated decision-making rules.
- **The right to compensation:** If any damage or distress is caused to the data subject due to the breach of the Act by the data controller, the data subject can claim compensation from the data controller.
- **The right to rectification and other remedies for inaccuracy:** Data subjects have the right to take action through a court to rectify, block, erase or destroy inaccurate data.
- **The right to ask the Commissioner to assess whether the Act has been contravened:** The data subject is also given the right to request the Information Commissioner to make an assessment if he or she feels that their personal information has not been processed in accordance with the Act.

9. Exemptions to Data Subject Requests

Not all personal data held by an institution will need to be disclosed upon request by a member of staff or student. There are several exemptions in the Act but these are applicable on a case by case basis. The exemptions below illustrate situations where an FE or HE institution can refuse to provide access to personal data.

- **Requested access to an examination script, other than examiners' comments:** This exemption allows an institution not to disclose the information concerning an academic, professional or other examination if such a request is made by a data subject. Also, it limits the freedom of the data subject in knowing their examination marks in advance of its general release.
- **Exemption relating to confidential references:** FE and HE institutions are exempt from furnishing to their employee copies of any confidential references written about them by the FE or HE institution.

10. Enforcement

The regulation and enforcement of the Act in the UK is done by an independent public body known as the Information Commissioners Office (ICO). The ICO provides guidance to organisations and individuals and has various rights of enforcement against data controllers who do not comply with the Act. If a data subject feels that a data controller has not complied with the Act then the data subject has:

- 1) the right to complain to the ICO who will then investigate and if needed serve an information notice or an enforcement notice in case of non-compliance. Appeal against the notices can be made to the Information Tribunal.
- 2) the right to sue the data controller

The Act also treats it as a criminal offence if

1. a data controller having received a subject access request destroys the data rather than disclose it.
2. a data controller discloses personal data without the authority to do so.
3. a data subject does not comply with an enforcement notice.
4. a data subject knowingly or recklessly obtains, discloses or procures the disclosure of personal information without the consent of the data controller.

Mahesh Madhavan

15 August 2007

Bibliography and References

The Data Protection Act 1998 available at
<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

Peter Carey, "*Data Protection Handbook*" (The Law Society) Edited by Peter Carey

Durant v Financial Services Authority (2003) EWCA Civ 1746, Court of Appeal (Civil Division) 2003 Court of Appeal

'*Data Protection and Freedom of Information: What they mean for you*', Records Management Section, University of Edinburgh power point presentation available at
<http://www.recordsmanagement.ed.ac.uk/InfoStaff/Training/Training.htm>

'*Data Protection Good Practice Note: Taking Photographs in Schools*', good practice notes issued by the Information Commissioners Office available at -
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_spec ialist_guides/taking_photographs_in_schools.pdf

'*Data Protection Good Practice Note: Subject Access and Employment References*', good practice note issued by the Information Commissioners

Office available at

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/subject_access_and_employment_references.pdf

'Loughborough University: Data Protection Policy' available at

<http://www.lboro.ac.uk/admin/ar/policy/dpact/ludpp.htm>

Graham Hadfield, 'Data Protection Overview' power point presentation available at

<https://www.redcar-cleveland.gov.uk/YrCounc1.nsf/Web+Full+List/B2BA9F34DA61BD6480256C8D003CAD4B?OpenDocument>

Peter Garrod, 'Data Protection and Freedom of Information: SOA'S Responsibilities, your Responsibilities' power point presentation available at -

<http://www.soas.ac.uk/about/index.cfm?navid=2646>

'Data Protection Act: Fact Sheet', guidance note issued by the Information Commissioners Office available at -

http://www.aimhigher.ac.uk/practitioner/resources/Data_protection_fact_sheet.pdf

Lancaster University Data Protection Project 2000 – 01 -

<http://www.dpa.lancs.ac.uk/>

Peter Garrod, 'Data Protection Workshop: How the law Affects you' power point presentation available at

<http://www.soas.ac.uk/about/index.cfm?navid=2646>

'SOAS: Data Protection Policy' available at

<http://www.soas.ac.uk/about/index.cfm?navid=2346>

Andrew Charlesworth 'Data Protection Overview', available at

<http://www.jisclegal.ac.uk/dataprotection/dataprotection.htm>

The Information Commissioners Office <http://www.ico.gov.uk>