

Data Sharing in FE and HE Administration

Andrew Charlesworth - Reviewed by Louise Townsend at Pinsent Masons

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.

20 December 2006

Table of contents

1. Data Protection Law – A Primer	1
2. Inter-Departmental Data Sharing	3
3. Data Sharing with Third Parties	5
4. Mandatory Data Sharing	7
5. Data Sharing and Freedom of Information	8
6. Summary	9

Introduction

This overview paper briefly explains the law relating to data protection and its application to the sharing of data, internally and externally, by Further and Higher Education (FE and HE) institutions. FE and HE institutions have a variety of reasons to want to share data, from increasing administrative efficiency, sharing information with law enforcement agencies through to sharing data with third parties who provide benefits to students and staff.

The Information Commissioner's Office (ICO) sees the ability to engage in data sharing as potentially highly beneficial to public sector institutions and intends to "...plac[e] less emphasis on narrow administrative law issues that have negligible data protection benefit for individuals ... [and] devote ... regulatory resources to addressing cases where the sharing of personal information results in genuine unfairness or unwarranted detriment to individuals". - ICO Policy Document -

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/sharing_personal_info_in_public_sector_new_approach.pdf.

The ICO is thus supportive of the reuse of data within broad categories of purpose, as long as appropriate data protection frameworks and safeguards are in place. In the case of FE and HE institutions, and their staff and students, effective data sharing should both reduce the time and cost overheads for all parties of the constant re-collection of data, and could also make gaining access to their personal data more efficient for individuals.

1. Data Protection Law – A Primer

In the UK the Data Protection Act 1998 (DPA 1998) provides the framework within which personal data can be lawfully used by individuals and organisations. It covers all

processing of personal data by FE and HE institutions, including computerised data, structured manual files and unstructured manual data, except where specifically exempted.

Where an FE or HE institution makes the decision to process personal data for a particular purpose and determines how it will be processed, they will be a Data Controller for that data. If an FE or HE institution holds or processes personal data, but someone else makes those decisions, the institution is acting as a Data Processor, and the third party is the Data Controller.

Personal data is information relating to a living individual who can be identified from it, or from it and other information held by, or reasonably accessible to, the Data Controller. A living individual who is the subject of personal data is referred to as a Data Subject.

Certain personal data is regarded as requiring particular protection, including:

- racial or ethnic origin,
- political opinions,
- religious beliefs,
- membership of trade union organisations,
- physical or mental health,
- sexual life,
- offences or alleged offences.

Such data is called sensitive personal data and stricter rules apply to its processing.

Data processing is defined very broadly in the DPA 1998. In most cases, from the moment personal data is collected, to the moment that it is destroyed or fully anonymised, the Act treats it as being processed. However, the definition of personal data can be interpreted more narrowly following the Court of Appeal decision in Durant v Financial Services Authority [2003] EWCA Civ 1746. For guidance on this case see ICO Guidance - http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf

The DPA 1998 describes the rights of Data Subjects and the obligations of Data Controllers when personal data is processed. It does not place direct obligations on Data Processors, but makes the Data Controllers who use them responsible for the processing their Data Processors carry out.

Data Controllers must always comply with eight enforceable principles of good information handling practice. These say that personal data must be:

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

Different Data Controllers may share personal data on Data Subjects. If they share the data for the same purpose they are 'Joint Data Controllers' and they will be jointly liable for any breach of the DPA1998 resulting from their processing. If they share the personal data for different purposes they are 'Data Controllers in common', and each remains individually responsible for their processing.

In most cases, data protection law does not explicitly bar data sharing either within an institution, or between an institution and other third parties. It does require that:

- processing of personal data, including sharing, has an identifiable and lawful purpose or purposes;
- the likely extent of the sharing is made known to the Data Subject - they should be made particularly aware of any 'non-obvious' purposes for which their information may be shared;
- adequate protections are in place to ensure that each Data Controller's obligations, and the Data Subject's rights, can still be met.

2. Inter-Departmental Data Sharing

Personal data about both staff and students that is directly, or indirectly, obtained by FE and HE institutions may often have a number of potential uses. Some of those potential uses may be barred by legal restrictions other than data protection law, such as disabilities discrimination legislation. If a use of personal data is not barred by other laws, then reuse and repurposing of data may be possible but only if data protection rules are observed. A common mistake is to assume that because personal data is held by a department within an institution, that it can thus automatically be shared with other departments or institutional employees "because we all work for the same institution."

The key elements to look at when considering sharing personal data are:

- Purpose - is there a clear and lawful purpose (or purposes) for the data sharing?
- Fairness - in the circumstances, is the nature and extent of the data sharing a proportionate means of achieving that purpose when weighed against the interests of the Data Subject?
- Transparency - has a degree of notice proportionate to the circumstances been provided in advance to Data Subjects about possible data sharing of their personal data?

It is important to remember that in order for a data controller to lawfully process non-sensitive personal data one of the following conditions must be met:

- 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

When data is shared, it is vitally important not to compromise the ability of Data Subjects to effectively exercise their rights under the DPA 1998, such as the right to access data which is held about them, and the right to object to, or opt out of, certain types of processing. Failure to provide adequate advance information about possible processing, including data sharing, may mean that it is considered to have been carried out unfairly and without due respect for the Data Subjects' rights.

Examples

Student A provides a set of personal data to the University of Bumbleside, comprising her address, telephone number and a non-University e-mail address. During her time at the University, the centrally held data will be used by the various parts of the institution, such as her department and the library, to contact Student A about issues relating to her studies. When she supplies the personal data, the University provides Student A with information about the purposes to which the data may be put. The data is not sensitive data, and the University may decide not to request consent to their processing, relying instead upon one of the other conditions. The use of Student A's personal data by the University for the provision of a variety of services to Student A, from a range of different academic and administrative departments, in connection with her course, can be seen to fall within a broad purpose.

At the end of her studies, the University of Bumbleside Alumni Office wishes to use the personal data in order to send out various offers and fundraising information to Student A. The purpose is now not in connection with Student A's course, it is essentially a marketing or fundraising exercise by the institution. The University has stated in its original information that the set of personal data will be supplied to the Alumni Office upon graduation, and it provides an opt-out for students who do not wish this to happen with their personal data. This would permit the sharing of the personal data collected in connection with administration of Student A's course with the Alumni Office for the purpose of marketing or fundraising. Student A is aware of the likely use of her data, she is able to object to that use, and so the University can pursue its legitimate interests without being unfair to Student A.

Candidate B applies to the University of Bumbleside, supplying a set of personal data including information about his disability. The data is sensitive personal data. The University has informed applicants of the purposes for collecting the data, which are that the University requires this data for statistical purposes, and in order to ensure that if the candidate is accepted on a course it makes such 'reasonable adjustments' as may be required under the Special Educational Needs and Disability Act 2001 (SENDA) to ensure

that Candidate B is not ‘substantially disadvantaged’. The data may be shared within the University only for the purpose of meeting those purposes, and as the data is sensitive personal data, the ability of the institution to share the data internally other than for those purposes, without Candidate B’s explicit consent, will be extremely limited. However, if the University identifies a need to share this data for wider purposes in advance of collection it can build in consent for these uses in its collection process.

3. Data Sharing with Third Parties

FE and HE institutions already share significant amounts of personal data about staff and students with other organisations. Some of that data sharing is required by law (see below), but much of it takes place in the context of the general operations of the institutions, primarily centred upon the provision or administration of educational services. As with intra-institutional data sharing, in many cases, data protection law does not stand in the way of data sharing with third parties, as long as the three requirements of purpose, fairness and transparency are met. When considering sharing data with third parties there are a number of issues to consider before the data sharing begins.

- Identifying the actors - who will be providing, obtaining, recording or holding the personal data that will be shared?
- Defining the purposes - what is the purpose of the data sharing, does it fall within the broad purpose for which the data was originally collected, or is it a new purpose?
- Determining data protection roles - will the third party with which data is to be shared be a data processor, a joint data controller, or a data controller in common? Do they understand the data protection implications of their role?
- Considering categories of personal data - is the scope of the personal data to be shared adequate, relevant and not excessive as regards the purpose?
- Identifying ‘sensitive personal data’ - is the personal data to be shared 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?
- Identifying the processing conditions - based on whether data is ‘sensitive’ or not, can the data sharing can be supported by one of the required processing conditions?
- Choosing processing conditions - If the purpose for the data sharing could be capable of justification under a number of the conditions, which condition is to be relied upon?
- Data subject consent - will data subject consent be required for the data sharing to be lawful? Has it been obtained? If not, how will it be obtained?

- Informing data subjects - Based on the information they were given when the data was collected, could the data subjects reasonably expect their personal data to be used for the purpose for which it is proposed to share it? Could they reasonably expect their personal data to be shared with the third party in question? Will they need to be informed of the data sharing by the third party?
- Data subject access - Have the data subjects been provided with sufficient information to exercise their data protection rights, including the right of access to data held on them? Can they identify the Data Controller or Controllers who will be sharing their data, and against whom their rights can be exercised?
- Contractual agreements between actors - Is the nature of the data sharing such that it would be sensible to have a formal agreement between the initial data controller and the third party? Should such an Agreement be a Data Sharing Protocol, a Joint Data Controllers Agreement or a Data Processor Agreement?
- Institutional Framework - Do the initial data controller and the third party have in place suitable practice and procedures to meet their data protection obligations?

Example

Freetown College wants to outsource the running of its virtual learning environment (VLE) to a private company, Alpha Systems. It will share certain non-sensitive personal data relating to its staff and students, for the purpose of populating the VLE with information necessary for Alpha Systems to support the College's educational service. As Freetown College is determining the purpose and nature of the processing, it is the Data Controller for that data - as Alpha Systems is not making decisions about the purpose and nature of the processing, it is a Data Processor on behalf of Freetown College. Freetown College is thus responsible under the Data Protection Act for the lawful processing of the personal data by Alpha Systems. It will be necessary for Freetown College to have sufficient oversight and audit powers built into its contractual arrangements with Alpha Systems to ensure it can meet its obligations as Data Controller.

Freetown College will need to ensure that the information it shares is adequate, relevant and not excessive for the purpose of running the VLE. As the data is non-sensitive personal data the College has a range of possible processing conditions available to it - data subject consent, performance of a contract with the data subject, legitimate interests of the data controller. The College decides that as the processing is to support the provision of educational services, and staff and students have been informed that the College may share their data with third party educational service providers for that purpose, the data sharing in this case does not justify the formality of collecting consent. It does, however, provide detailed information to its staff and students in advance of sharing the data, noting that it remains the Data Controller for their personal data. It also makes provision for them to discuss the sharing with College officials, and present any objections.

The above example is a simple scenario for data sharing. A good example of a much more complex third party data sharing arrangement can be seen in the data protection background documentation for the Union Education Online project - <http://www.tuc.org.uk/extras/UEODataFlows.pdf> and the JISC document Data Protection, Lifelong Learner Record Systems & ePortfolios: A Short FAQ - http://www.jisc.ac.uk/uploaded_documents/Data_Protection_FAQ.pdf.

4. Mandatory Data Sharing

The DPA 1998 itself does not oblige institutions to disclose personal data to specific third parties, but states that personal data are exempt from the Act's 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 can thus require disclosure of an individual's personal data by an institution. Institutions should, however, where possible, ensure that staff and 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. Examples of third parties who may require disclosure by an institution are included in the following table.

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. In other cases the section 29 exemption in the DPA 1998 may be appropriate where the disclosure is necessary for specified purposes.
Other third parties	Court Order - e.g. third party disclosure order.

Example

The Child Support Act 1991 (CS Act) provides the system for child maintenance in Great Britain, operated by the Child Support Agency (CSA). The CSA collects information to enable it to deal with applications for child maintenance, including information that will help to trace non-resident parents; calculate maintenance; and enforce maintenance liability.

Lecturer D is newly employed by Freetown College. Previously married, he is a non-resident parent (NRP) with two children for whom he is supposed to make regular child maintenance payments. He has not informed the CSA of his new employment, and is in arrears with his payments.

The CS Act allows the CSA to obtain specific information from certain people and organisations. These include the employers of non-resident parents. The CSA sometimes uses inspectors to gather information. They can visit the place where a non-resident parent works to collect information. It is a criminal offence if any person or organisation required by law to supply information to the CSA fails to do so, or intentionally delays or obstructs inspectors doing their job.

An inspector calls at Freetown College on the basis of information that Lecturer D is now working there. The inspector wants to confirm that Lecturer D is an employee of the College and, if so, will also require details of Lecturer D's employment and pay.

If the College refuses to co-operate and share the relevant data with the inspector, it is committing a criminal offence and may be fined up to £1000. As the disclosure is a legal obligation, the College does not require permission from Lecturer D to disclose the information, nor does it matter that Lecturer D objects to his information being disclosed to the CSA. The College should, however, ensure that it has made reasonable efforts to verify that the requestor is in fact a CSA inspector. The College may wish to make clear to its employees in advance that, in certain circumstances, it is obliged by law to disclose their personal data.

5. Data Sharing and Freedom of Information

FE and HE institutions should be aware that when sharing personal data, this may occasionally have implications beyond the field of data protection. It may be possible in some circumstances that sharing data with third parties that contains both personal data elements and non-personal data elements may also open up issues of whether the third party is holding information on behalf of the institution which is subject to disclosure under the Freedom of Information Act 2000 (FOIA 2000). For more information on FOIA 2000 see the JISC Legal FOIA publications page -

<http://www.jisclegal.ac.uk/freedomofinformation/freedomofinformationPub.htm>

Example

A private company, PlagaStop, offers to provide plagiarism detection services to the FE and HE sector. An institution will submit copies of candidates' assessed work, accompanied by identifying student data (name, email address, course details and institution) to the private company who will use a computer system to check the assessed work against a database of existing assessed work and other publicly available materials.

The agreement between the submitting institution and PlagaStop is that the submitting institution remains the Data Controller for the personal data submitted. The stored student essay is not in itself personal data and the DPA 1998 would not apply to it.

Once the assessed work and the personal data are submitted to PlagaStop, they are both held in perpetuity, unless the submitting institution requests that they be removed, or stops subscribing to the service. A student may object to the holding of the personal data, but the private company will only act on receipt of a s.10 DPA 1998 notice, and only then where there is evidence of substantial and unwarranted damage or distress. It is explicitly stated that this is not a general right for students to withdraw data.

The purpose of the retention is two-fold. If plagiarism is detected, an 'audit trail' of the document plagiarised may be established between author and plagiariser, e.g. where there are clusters of plagiarism from a particular document. Also in certain cases, the work may be legitimately submitted at different institutions by the same student e.g. if the student started at Institution A, dropped out and went to study at Institution B.

If the personal data remains connected to the stored essay, and the submitting institution remains the Data Controller, it is arguable that the essay can be linked to the submitting institution sufficiently that it can be said that PlagaStop is holding both personal data and essay on behalf of the submitting institution. The submitting institution will be a Public Authority for the purposes of FOI but PlagaStop is not a Public Authority. If an individual wanted to make an FOI request for one or more essays (perhaps using PlagaStop as a form of digital repository for their own work, or as a research tool) they cannot make it directly to PlagaStop, but they could make it to the submitting institution, as PlagaStop is holding the relevant (and still identifiable data) on their behalf, even if the institution itself has destroyed all copies of the assessed work in accordance with its data retention schedule. If an FOI request is received the institution would thus be under an obligation to consider this and possible retrieve the data from PlagaStop, although exemptions from disclosure may be available

Stripping off the personal data would make it difficult for the stored essay to be identified, would end the submitting University's role as Data Controller, and arguably break the chain of 'ownership' between the University and the stored essay, also ending the FOI obligation.

6. Summary

FE and HE institutions may wish to share personal data both internally and externally for a variety of reasons.

In summary, the DPA 1998 does not explicitly bar data sharing. However it does provide a legal compliance framework within which any data sharing must take place. Institutions should also consider whether any other laws, such as the law of confidence, have an impact on their proposals.

Andrew Charlesworth - Reviewed by Louise Townsend at Pinsent Masons

20 December 2006