Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998
Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998

Please note: this guidance is supplied by JISC Legal for information purposes only and is not, nor is it 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.

Please note: The previous version of this Code of Practice is now archived on the JISC website at - http://www.jisc.ac.uk/publications/publications/

Andrew Charlesworth

09 May 2008

© JISC Legal - www.jisclegal.ac.uk
Table of Contents

Foreword and Acknowledgements 5
Introduction 6
1. Key Concepts 7
   1.1 Purpose 7
   1.2 Fairness 7
   1.3 Transparency 7
2. Key Definitions 8
   2.1 Data 8
   2.2 Personal Data 8
   2.3 Sensitive Personal Data 9
   2.4 Data Subject 9
   2.5 Data Controller 9
   2.6 Data Processor 10
   2.7 Data Processing 10
   2.8 Data Processing Agreement 10
   2.9 Fair Processing Notice 10
   2.10 Consent 10
   2.11 Legitimate Interests 11
3. Interaction with Other Legislation 12
   3.4 Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003) 14
   3.5 The Electronic Commerce (EC Directive) Regulations 2002 15
   3.6 Other Legislation 15
   Table 1: Categories of Personal Data in the DPA 1998 after FOIA 2000 Amendments 16
4. Privacy Impact Assessment 17
   4.1 General 17
   4.2 Why Carry Out a PIA? 17
   4.3 When Should a PIA be Carried Out? 18
   4.4 Who Should Be Involved in a PIA? 18
   4.5 Further Guidance 18
5. Use of Personal Data by Employees 19
   5.1 Processing Under an Institutional Notification 19
   5.2 Processing Outside an Institutional Notification 19
   5.3 Employee Access to, and Use of, Personal Data 19
6. Use of Personal Data by Students

6.1 Processing by Students where the Institution is the Data Controller

6.2 Processing by Students where the Institution is not the Data Controller

6.3 Student Access to, and Use of, Personal Data

7. Data Sharing

7.1 General

7.2 Intra-Institutional Data Sharing

7.3 Data Sharing with Third Parties

7.4 Disclosure Under s.28 & s.29 DPA 1998: National Security, Crime and Taxation

7.5 Disclosure to Employees under Discrimination Legislation

7.6 Mandatory Disclosures

7.7 Verification of Student Attendance and Qualifications

7.8 Reports to Parents and Sponsors

Table 2: Examples of Third Parties who can require Disclosure of Personal Data

7.9 Disclosure to the Border and Immigration Agency (BIA)

7.10 Other Disclosure Issues

7.11 Provision of Guidance

University of Edinburgh, Guidelines on disclosure of information about students (Jan 2008)

8. Security of Personal Data

8.1 Institutional Framework for Data Security

8.2 Employee Security, Training and Management

8.3 Vendors, Contractors, and Suppliers

8.4 Students

8.5 Transfer of Personal Data

8.6 Migration or Upgrade Plans

8.7 Back-up of Personal Data

8.8 Processing of Personal Data Off-site

8.9 Disposal of Data

9. Examinations

9.1 Examination and Assessment Process

9.2 Examination Scripts

9.3 Examiners’ Comments

9.4 Automatic Processing

9.5 Examination Board Minutes and Related Documentation

9.6 Disclosure of Results
10. Use of Personal Data in Research

  10.1 General
  10.2 Online Research with Human Subjects
  10.3 Provision of Research Data to 3rd Parties

11. References

  11.1 References Given by FE and HE Institutions
  11.2 References Received by FE and HE Institutions
  11.3 References Internal to FE and HE Institutions

12. The Internet and Online Services

  12.1 Institutional Web pages
  12.2 Institutional Staff and Student Directories
  12.3 Web pages Used to Collect Personal Data
  12.4 Personal Employee and Student Web pages on Institutional Machines
  12.5 Internet and Intranet Monitoring
  12.6 Web 2.0 Services
  12.7 e-Learning Systems - Virtual Learning Environments, ePortfolios

13. Collection and Processing of Personal Data Relating to Disability

14. Other Information

  14.1 Next of Kin/Emergency Contact Information
  14.2 Counselling Services
  14.3 Careers Services
  14.4 Applications for Access Funding and Other Discretionary Funding
  14.5 Alumni Records
  14.6 CCTV and Similar Surveillance Equipment
  14.7 Student Unions

15. International Transfers of Personal Data

  15.1 Transfers of Personal Data to EEA Countries
  15.2 Transfers of Personal Data to Non-EEA Countries
    15.2.1 Formal Adequacy Rulings
    15.2.2 Schedule 4 DPA 1998 Derogations
    15.2.3 Use of Model Clauses or Binding Corporate Rules
    15.2.4 Data Controller Assessment of Adequacy


  16.1 In Scotland & Northern Ireland
  16.2 To Individuals Under the Age of 18
  16.3 To Foreign Nationals

17. Retention of Records Containing Personal Data

Glossary and Acronyms
The Code of Practice for the Higher and Further Education Sectors on the Data Protection Act 1998 was initially written in early 2000, with a second draft, taking into account feedback from the FE and HE Community, produced in December 2000. This third version was commissioned by JISC Legal in November 2007, to update the Code of Practice to take into account developments in legislation, case law and technology that have occurred in the intervening seven years.

Acknowledgements should be paid to the following people involved in the development of the Code of Practice over the years: Rosemary Jay, Lucy Inger, Linda Malloy, Adrian Tribe, Dr. Trevor Field, Jane Williams, Sally Justice, John Hitches, Anne Johnson, Dr. John M Gledhill, Andrew Cormack, Maurice Frankel, Anne Kipling, Mike Davies, Ann Jones, Samantha Hill, Dr. Stuart Hannabuss, Victoria Cranna, Rachael Maguire, Ann McGeachy, Gareth Davies, Susan Graham, and the team at JISC Legal. Additionally, the section on Web 2.0 technologies draws heavily upon the University of Edinburgh’s Guidelines for Using External Web 2.0 Services.

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

Andrew Charlesworth
Senior Research Fellow & Director, Centre for IT & Law
University of Bristol
Wills Memorial Building
Queens Road
Bristol BS8 1RJ

A.J.Charlesworth@bristol.ac.uk - May 2008
The following Code of Practice is designed to provide guidance to the FE and HE sectors on issues of specific relevance to their day-to-day operations. As such, the Code of Practice does not provide an in-depth examination of the general principles of the Data Protection Act 1998, which are widely available elsewhere, but concentrates on key issues of concern to FE and HE institutions. Where guidance notes for specific aspects of the handling of personal data are available from the Office of the Information Commissioner (OIC), as is the case with employer/employee relations, CCTV, and transfers outside the EU/EEA, this Code of Practice will refer readers to them - http://www.ico.gov.uk/.

It should be noted that the Code of Practice is intended to be a guide to best practice in this area, and is not designed to be mandatory or prescriptive in nature. FE and HE institutions may thus decide to adopt data protection practices that differ from those suggested here according to their particular circumstances.
The first thing to note when reviewing the implications of the Data Protection Act 1998 for the FE and HE sector is that in many ways the term ‘data protection’ is something of a misnomer. Data protection or data privacy regimes, such as that required by the EU Data Protection Directive, do not seek to protect data itself, rather they seek to provide the individual with a degree of control over the use of their personal data, most notably unforeseen secondary uses of that data, and to provide protection from unwanted or harmful uses of personal data. As such, data privacy regimes do not seek to cut off the flow of data, merely to see that it is collected and used in a responsible and, above all, accountable, fashion. To achieve this aim successfully, there are three key concepts which data controllers should always have in mind when considering a new processing operation.

1.1 Purpose

The first and most basic tenet underlying the Act and its various concrete provisions is that of Purpose. Data controllers are required by the Act to process personal data only where they have a clear and legitimate purpose for doing so, and then only as necessitated by that purpose. A data controller’s purpose for any personal data processing operation should thus be clearly identified and set out in advance of the processing, and should be readily demonstrable to data subjects.

1.2 Fairness

As noted above, the DPA 1998 is not intended to be an absolute obstruction to processing of personal data. Both the legislation, and the Information Commissioner, recognise that there are many legitimate purposes for the processing of personal data, even where data subjects may not wish this to happen. The essential element here is that of ensuring fairness in the relationship between data controller and data subject. Thus, where a data controller has identified a particular purpose for processing of personal data, they must also consider its fairness. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation, for many others, data controllers will need to make their own determination as to the requirements that will have to be met for processing to be deemed fair. This determination may be based solely on the data controller’s interpretation of the DPA 1998, or in conjunction with advice from the Information Commissioner, sectoral practice, or rules laid down by the courts. Ideally, data controllers will take as broad an approach as possible to their fairness criteria in assessing each processing operation; as such an approach will reduce the likelihood of data subject discontent with that processing.

1.3 Transparency

It is clear from the DPA 1998 that much of the onus for ensuring effective enforcement of their rights will lie with the data subject. To that end, the Act requires data controllers to provide data subjects with a basic minimum amount of information about the collection, use, and distribution of their personal data. Data subjects thus need to know the purpose of the processing, and the measures that the data controller has taken to ensure that the processing is fair. Transparency of the data controller’s operation is thus the final element of the regime – who will be processing the data, how will it be processed, and to whom will it be disclosed. For many types of data processing it will not be unduly onerous, or indeed harmful to operations, for data controllers to provide more information than the statutory minimum. The more transparent a data processing operation is to data subjects, the less likely it is that they will feel the need to make subject access requests to elicit further information.
2. Key Definitions

2.1 Data

'Data' falling under the DPA 1998 is defined as information which:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
- Is not covered by the first two categories but forms part of an 'accessible record':
  - a health record consisting of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual
  - an educational record processed by or on behalf of the governing body of, or a teacher at any school in England and Wales which relates to any person who is or has been a pupil at the school, and originated from or was supplied by or on behalf of an employee of the local education authority which maintains the school; a teacher or other employee at the school; the pupil to whom the record relates; a parent of that pupil
  - any accessible public record which is kept by an authority specified in Schedule 12 of the DPA 1998
- Is recorded information held by a public authority and does not fall within any of the previous categories

However, the recent Court of Appeal decision in Johnson v Medical Defence Union Ltd [No 2] (2007) has added a degree of confusion to this definition, as it was held in that case (on a split decision, 2-1) that the selection of information from various manual and electronic files and its compilation in a computer-created document was not the creation of data capable of being processed – a holding that appears inconsistent with the wording of the Data Protection Directive 1995 (DPD 1995). Regardless of the Johnson decision, the fact that FE and HE institutions are legally considered to be public authorities for the purpose of this definition means that it would be sensible for institutions to construe the definition of 'data' broadly.

2.2 Personal Data

'Personal data' is defined in the DPA 1998 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 DPD 1995 further defines an identifiable person as one who can be identified by reference to 'an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

The meaning of the term ‘personal data’ was considered 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:

- "The first is 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 appears together with other information about the named individual such as address, telephone number or information regarding his hobbies.

The definition of ‘personal data’ in the Durant case has since been followed in Johnson v Medical Defence Union (2007) and Smith v Lloyds TSB Bank plc (2005).

More recently, in the light of an Opinion of the Article 29 Working Party (Opinion 4/2007 on the concept of personal data (01248/07/EN – WP136) 20 June 2007), the Information Commissioner’s Office (ICO) released new guidance on how the data controller should determine whether or not particular forms of data are ‘personal data’.

‘Personal data’ is likely to be processed where:

- A living individual can be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the data controller
  o identification by name is an obvious example, but even where a name is not known, an individual may be capable of identification from amalgamated data
- The data ‘relates to’ the identifiable living individual, whether in personal or family life, business or profession
  o e.g. the data is ‘obviously about’ a particular individual
  o e.g. the data is ‘linked to’ an individual so that it provides particular information about that individual
- The data is used, or is to be used, to inform or influence actions or decisions affecting an identifiable individual
- The data has biographical significance in relation to the individual
- The data focuses or concentrates on the individual as its central theme rather than on some other person, or some object, transaction or event
- The data impacts or has the potential to impact on an individual, whether in a personal, family, business or professional capacity


2.3 Sensitive Personal Data

The DPA 1998 defines sensitive personal data as 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.

2.4 Data Subject

The DPA 1998 defines a Data Subject as a living individual who is the subject of personal data. Dead people cannot be data subjects, nor, in the UK and most other EU Member States, can ‘legal individuals’, such as companies.

2.5 Data Controller

The DPA 1998 defines a Data Controller as “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. This is probably one of the most widely misunderstood definitions in the Act.

- 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. The term does not appear to be widely used
- 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’
2.6 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. It states that Data Controllers must place their relationship with a Data Processor on a written contractual basis. The contract must require the data processor to act only on instructions from the Data Controller, and to comply with obligations equivalent to those imposed on a data controller by the seventh principle (appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data). Data Controllers thus need to ensure that their relationship with a Data Processor is governed by a formal Data Processing Agreement.

2.7 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, organisation, 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 has meant that many authorities have considered 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. This common understanding is potentially undermined in some circumstances by the decision in Johnson v Medical Defence Union Ltd (No 2) (2007), noted above, relating to the definition of ‘data’ falling under the DPA1998. However, it is suggested that, as regards FE and HE institutions, the breadth of the definition of ‘data’ applying to ‘public authorities’ means that institutions would be wise to continue to observe that position.

2.8 Data Processing Agreement

A Data Processing Agreement means a contract between a Data Controller and a Data Processor, which will be entered into before the Data Processor begins processing personal data on behalf of the Data Controller, and which set out the responsibilities of both parties in respect of that processing, as well as any indemnities required by the parties.

2.9 Fair Processing Notice

A fair processing notice is used by a Data Controller to provide a Data Subject with information relevant to the processing of their personal data, usually at the time of its collection. It will describe the purposes for which the Data Controller intends to process their personal data, and should also include details of Joint Data Controllership, as well as indications of third parties to whom the data may be disclosed or transferred, and the purposes served by those transfers or disclosures. As such, the fair processing notice does not need to cover every specific eventuality, but must provide sufficient information to demonstrate that a Data Subject could have ‘reasonably expected’ their data to be processed in the manner the Data Controller intends. The fair processing notice should provide enough information to the Data Subject to allow them to utilise effectively the rights provided to them by the DPA 1998 (e.g. subject access). The Data Subject should be able to re-access the fair processing notice at a later date in hardcopy or electronic form. Changes to a fair processing notice should always be notified to relevant Data Subjects.

2.10 Consent

The DPA 1998 does not contain a definition of ‘consent’ or ‘explicit 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). Additionally, for ‘explicit consent’ to be relied on to provide a Sch.3 criterion (Sch.3, s.1) for lawful processing, some clear form of affirmative action (e.g. written consent, clicking on an ‘I accept’ button on a webpage) is likely to be required. 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 the legitimate interests of the Data Controller or a third party, would be more practical.

2.11 **Legitimate Interests**

The DPA 1998 Sch.2 s.6 allows, as a criterion for lawful processing of a Data Subject’s personal data, the fact that the processing is necessary for the purposes of legitimate interests pursued by the Data Controller, or by a 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. This criterion applies to circumstances where the personal data to be processed does not contain sensitive personal data. Where sensitive personal data is to be processed, the Data Controller must satisfy both a Sch.2 and a Sch.3 criterion and, as legitimate interests of the Data Controller or a third party is not a listed criterion for lawful processing under Sch.3, an additional Sch.3 criterion will be required. Many circumstances where non-sensitive student data is processed and/or disclosed by FE and HE institutions will be capable of legitimisation as lawful processing under the criterion of legitimate interests, for example, the submission of data to the National Student Survey.
3. Interaction with Other Legislation


The Freedom of Information Acts give a general right of public access to all types of ‘recorded’ information held by public authorities, set out exemptions from that general right, and places a number of obligations on public authorities. The Acts only apply to ‘public authorities’ and not to private entities. Public authorities, as defined in the Acts include schools, colleges and universities. The FOI Act 2000 only applies to England, Wales and Northern Ireland. The UK Information Commissioner’s Office (ICO) oversees both the Freedom of Information Act 2000 and the Data Protection Act 1998. Both Acts relate to aspects of information policy. They overlap where personal information is considered for disclosure. There is a separate Freedom of Information Act for Scotland. The Scottish Information Commissioner oversees FOI in Scotland but the ICO oversees DP in Scotland. Public authorities have two main responsibilities under the Acts:

- They must produce a ‘publication scheme’, in essence, a guide to the information they hold which is publicly available
- They must deal with individual requests for information. Under the DPA 1998 individuals have a subject access right as regards their personal data, held on computer, and in some paper files. The FOIA and FOISA additionally permit individuals to request all other types of information that public authorities hold, subject to specific exemptions in the Acts

The FOIA 2000 also extends the data subject access rights that already existed under the DPA 1998, to include all “recorded information held by a public authority” not otherwise covered by the DPA 1998 [in other words, any personal data not held on computer or in a relevant structured manual filing system]. This extension also applies to Scotland. The FOIA 2000 states that information is “held” by a public authority if:

- It is held by the authority, otherwise than on behalf of another person, or
- It is held by another person on behalf of the authority

While the FOIA 2000 amendments to the DPA 1998, in principle, make all personal data held by FE/HE institutions available to data subjects, regardless of the form in which it is held, there are important limitations upon the rights granted:

- Recorded information held in manual form outside of ‘relevant structured manual filing systems’ by FE/HE institutions is exempt from all of the data processing principles and obligations, apart from the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress
- There is a partial exemption from the subject access provisions for the new category of data. This exemption is provided by dividing the new category of information into ‘structured’ and ‘unstructured information’; and restricting access to the “unstructured information” to that which is described by the data subject and falls within specific costs limits
- A final exemption for the new category of data absolutely exempts personnel matters (i.e. information about “appointments or removals, pay, discipline, superannuation or other personnel matters”). However, the fact an exemption exists under the DPA 1998 does not mean that FE/HE institutions have to use it. Some institutions may opt for more open practices, for example in relation to personnel records

A request by an individual for information about him or herself is exempt under the two FOI Acts 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 third party information. Any information about an individual that is exempt from disclosure to them under the DPA 1998 is also exempt under the FOI Acts, subject to consideration of the public interest by the institution (qualified exemption).

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, the request falls within the remit of the FOI Acts. However, the authority must a
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.


- Makes it unlawful for a public authority, such as a government department, local council or the police to breach the European Convention on Human Rights, unless an Act of Parliament meant it could not have acted differently
- Permits individuals bringing an action for alleged breach of their rights to have the case heard by a UK court or tribunal rather than having to go to the European Court of Human Rights in Strasbourg
- Requires UK legislation to accord with the rights set out in the Convention

The main provision of the HRA 1998 relevant to data protection is Article 8, which reads:

- Everyone has the right to respect for his private and family life, his home and his correspondence
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

The Act is designed to apply human rights guarantees beyond the obvious governmental bodies. s. 6 HRA 1998 identifies two distinct categories of “public authorities” which would have a duty to comply with the Convention rights:

- “Pure” public authorities (such as government departments, local authorities, or the police) are required to comply with Convention rights in all their activities, both when discharging intrinsically public functions and also when performing functions which could be done by any private body. s.6(3)(a)
- “Functional” public authorities who exercise some public functions but are not “pure” public authorities are required to comply with the Convention rights when they are exercising a “function of a public nature” but not when doing something where the nature of the act is private. s.6(3)(b)

Only those bodies which fall within either of these categories (“pure” or “functional” public authorities) have a direct obligation under the Act to comply with Convention rights. The precise nature of particular FE and HE institutions under these categories appears to remain unclear – unlike the FOIA 2000, the HRA 1998 contains no listing of either ‘pure’ or ‘functional’ public authorities.

However, from a data protection point of view, in circumstances where an FE or HE institution was not directly breaching the HRA 1998, UK courts are required to comply with Convention rights, and obliged to interpret legislation in accordance with Convention rights. Therefore, breaches of the DPA 1998 could give an indirect cause of action to individuals seeking to claim that their Article 8 rights were being breached. As such, FE and HE institutions should be aware that the requirement of respect for private and family life, home and correspondence under Article 8 will influence judicial interpretations on DPA 1998-related issues such as the protection of personal information and the right to private communications. Any interference with the right must be in legitimate pursuit of fair and lawful purposes and must be demonstrably necessary and proportionate to achieve those purposes.
It should be noted that the HRA 1998 may require an institution to balance an individual's claims for breach of privacy or misuse of private information under Article 8 ECHR against countervailing arguments based on the Article 10 ECHR rights relating to freedom of expression, including the freedom to receive and impart information and ideas. Post HRA 1998, there are increasing signs that the courts are moving away from a 'public interest' test where those seeking to publish information of a private nature would need to show that there were exceptional circumstances which required its disclosure, to a test of whether a fetter on the right of freedom of expression in the circumstances surrounding that disclosure is “necessary in a democratic society” - Prince of Wales v Associated Newspapers (2006).


The Regulation of Investigatory Powers Act 2000 (RIPA 2000) provides, in conjunction with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR 2000), grounds for the lawful interception of communications, including telephone and computer communications (e.g. e-mail, instant messaging). However, personal data collected under the RIPA and the LBPR must be processed in accordance with the requirements of the DPA 1998, unless elements of that processing are specifically exempted e.g. processing of personal data collected under the RIPA/LBPR for the purposes of law enforcement (s.29, DPA 1998) or national security (s.28, DPA 1998) is exempted from parts of the Act.


The Privacy and Electronic Communications Regulations regulate direct marketing activities by electronic means (by telephone, fax, email or other electronic methods). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and ‘spy ware’. The Regulations complement the DPA 1998 in the regulation of organisations’ use of personal data and in ensuring appropriate safeguards for individuals’ rights and privacy. The Regulations apply different rules to individual subscribers and corporate subscribers, although some rules apply to both. Where personal data is used the DPA 1998 always applies, and the Regulations cannot be used to avoid the requirements of the DPA 1998.

‘Direct marketing’ means ‘the communication [by whatever means] of any advertising or marketing material which is directed to particular individuals’ [s.11 DPA 1998]. The ICO considers “direct marketing” as covering a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation’s aims and ideals.”

Where an institution wishes to communicate via electronic means with individuals, such as prospective students [e.g. marketing the institution] or alumni [e.g. fundraising] they must comply with the following rules:

- In order to use automated calling systems for marketing communications to individual subscribers the institution must have prior consent. Prior consent means that the individual has given some positive indication of intention; this does not necessarily require a tick box “opt-in” e.g. if the individual has clearly indicated their consent to the purposes and to the receipt of marketing communications in some other fashion i.e. clicking on an “Accept” button at the end of a marketing notice
- In order to use faxes for marketing communications to individual subscribers the institution must have prior consent, and check with the Fax Preference Service on a regular basis, unless the individual has notified the institution that such communications can be sent 'for the time being'
- In order to use live voice telephone calls for marketing communications to individual subscribers the institution must honour individuals’ “Do not call” requests, and check with the Telephone Preference Service on a regular basis, unless the individual has notified the institution that such communications can be sent ‘for the time being’
In order to use e-mail/SMS for marketing communications to individual subscribers the institution must have the opt-in consent of subscribers OR meet the soft-opt-in test:

- Contact details are obtained during negotiation or sale of goods or services to the recipient AND
- Marketing is conducted by the same entity as previous dealings with the individual AND
- Marketing relates to “similar products and services” AND
- An opt-out mechanism is provided at the point of data collection and is provided with each new communication

The Privacy and Electronic Communications Regulations are enforced by the Information Commissioner’s Office (ICO). If the Information Commissioner finds a business to be in breach of the Regulations Information Notice requesting further information an Enforcement Notice will be issued. A fine may be imposed for breach of an Enforcement Notice.

3.6 Other Legislation

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 in order to meet other legislative requirements. Examples of such legislation can be found in the section on Disclosure to Third Parties below.

Institutions should, where possible, ensure that staff and students are properly warned of any known statutory disclosures that they are likely to be 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.
<table>
<thead>
<tr>
<th>Category of Personal Data</th>
<th>Definition</th>
<th>Exemptions from DPA 1998</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant filing system (All data controllers)</td>
<td>Personal data recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. Files structured/referenced so as to clearly indicate 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. System 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 is readily accessible.</td>
<td>Relevant general exemptions and exemptions in secondary legislation. Exempt from most data processing principles and obligations EXCEPT the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress. Personnel information contained in manual records held by a public authority is absolutely exempt from DPA 1998.</td>
</tr>
<tr>
<td>Accessible record as defined by s. 68 DPA (All data controllers)</td>
<td>Health record [defined by s.68 ss. (2) DPA] Educational record [defined by Sch. 11 DPA] Accessible public record [defined by Sch. 2. DPA]</td>
<td>Relevant general exemptions and exemptions in secondary legislation. Exempt from most data processing principles and obligations EXCEPT the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress. Personnel information contained in manual records held by a public authority is absolutely exempt from DPA 1998.</td>
</tr>
<tr>
<td>Structured form (Public authorities only)</td>
<td>Personal data that forms part of a collection of information that is coherent enough to be classed as a “set of information”. Structured information does not have to be “readily accessible”.</td>
<td>Relevant general exemptions and exemptions in secondary legislation. Exempt from most data processing principles and obligations EXCEPT the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress. Personnel information contained in manual records held by a public authority is absolutely exempt from DPA 1998.</td>
</tr>
<tr>
<td>Unstructured form (Public authorities only)</td>
<td>Any personal data not falling into the first 4 categories.</td>
<td>Relevant general exemptions and exemptions in secondary legislation. Exempt from most data processing principles and obligations EXCEPT the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress. Personnel information contained in manual records held by a public authority is absolutely exempt from DPA 1998. Must be described by the data subject sufficiently to enable the authority to identify the specific information in question, and the subject access provisions will be subject to the cost limits under the FOIA. NB This does not mean that FE/HE institutions can charge more than £10 for a SAR for unstructured data, but that if the determination of the estimated cost of complying is over £450 then they can refuse to comply with the request.</td>
</tr>
</tbody>
</table>
4. Privacy Impact Assessment

4.1 General

Institutions considering adopting new administrative systems and other processes with possible privacy implications, or updating existing systems or processes (such as student record systems, virtual learning environments [VLEs], ePortfolio systems and distance learning programmes) should consider undertaking a Privacy Impact Assessment (PIA) in the early stages of project or process design, well before roll-out/implementation.

Privacy Impact Assessment can be defined as a process whereby a project’s potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a constructive search is undertaken for ways to avoid, minimise or at least ameliorate privacy concerns. PIAs are most effective when they are:

- Applied to initiatives under development, at a time when the personal information aspects are known, but before key development, system design, and operational decisions are set in stone and become costly to change
- Part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of threat/risk assessment

PIAs are not compulsory for public or private sector organisations under data protection law in the UK, but are carried out voluntarily by a diverse range of public and private sector organisations, including government departments, banks, and telecommunications companies.

4.2 Why Carry Out a PIA?

There are many reasons for undertaking a PIA exercise. The potential for privacy risk will be dictated by the nature of the initiative under consideration, and the context within which it is introduced. There can be no automatic “triggers” which can replace the exercise of human judgment. Key reasons are likely to be:

- Identification and Management of Risks - Projects that give rise to privacy concerns generally involve considerable financial investment. Senior management are responsible for ensuring that risks are identified, assessed, and managed. If privacy issues represent a barrier to realisation of the intended benefits, they need to be assessed, and a risk management plan devised and implemented. Thus, a PIA is a means of identifying and addressing an element of project risk within a broader risk management strategy at project management levels, whilst generating information to aid decision-making, and supporting good governance and business practices at senior levels of organisations
- Cost Avoidance - By performing a PIA early in a project, an organisation avoids problems being discovered at a later stage, when changes and the ‘retrofitting’ of features are much more expensive. The PIA process of articulation of a project’s objectives, the organisation’s requirements, and the justifications for particular design features will also have important benefits for general project management. Building privacy-sensitivity into the design from the outset also provides a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer life for the application
- Avoidance of Loss of Trust and Reputation - A PIA is a way to ensure that systems are not deployed with privacy flaws that will attract the attention of the media, public interest advocacy groups or regulators, or give rise to concerns among data subjects
- Meeting and Exceeding Legal Requirements - Data protection compliance checks and privacy audits ensure that an organisation addresses the informational aspects of privacy. Meeting such requirements is essential to avoid loss of trust and reputation. However, where a project affects wider dimensions of privacy, such as privacy in communications or physical privacy, it will be to an organisation’s advantage to define the scope of the PIA to extend beyond information privacy and explore how such privacy issues can be identified and addressed in innovative and publicly visible ways
4.3 When Should a PIA be Carried Out?

Ideally, the PIA process should begin early to ensure that project risks are identified and appreciated before problems become embedded in the design. This will usually mean commencing a PIA as part of the Project Initiation Phase. If the project is already under way, the PIA should be started as soon as possible so that any major issues are identified with the minimum possible delay. A PIA can be conceived and conducted as a one-time activity. In such circumstances, the PIA will take into account the information available about the project at the time, and feed ideas forward into the design. Yet this type of PIA cannot reflect information, often of a more detailed nature, that may become available at a later stage in the project. In major projects, thus the most beneficial and cost-effective approach may be to conceive of the PIA as:

- A cyclical process
- Linked to the project’s own life-cycle
- Re-visited in each new project phase

Most organisations use an initial screening tool to determine:

- Whether a PIA needs to be completed and
- The scale of the PIA to be conducted

A screening tool also allows appropriate resource allocation commensurate with the privacy risks. The Information Commissioner’s Office has developed a screening tool, as part of its PIA Handbook.

4.4 Who Should be Involved in a PIA?

Programme or business areas usually have responsibility for producing the PIA but draw on a variety of expertise. PIAs are often completed at the senior analyst level or by a manager with ongoing programme administration responsibilities. A team or committee approach is often found to be effective and brings a wider range of expertise into the PIA process. This can include, with varying degrees of participation:

- Programme and project managers
- Privacy policy advisors
- Legal advisors/legal officers
- Records management staff
- Information technology or data security experts
- Communications staff
- Other functional specialists, as appropriate

The use of external consultants can bring some advantages, including provision not just of expertise, but also independence and credibility, and may be particularly valuable for institutions with no internal privacy expertise and/or a small administrative staff. It is likely, however, that the best balance, and the best outcomes for the institution and the privacy interest alike, may be achieved by having the process managed by internal staff with sufficient expertise, seniority and independence, supplemented by external consultancy support.

4.5 Further Guidance

Guidance on PIAs, including advice on when a PIA should be carried out, who should be involved, and what form the process might take, is available from the ICO website at:
5. Use of Personal Data by Employees

5.1 Processing Under an Institutional Notification

Where employees at FE and HE institutions are processing personal data, for which their employer is Data Controller, 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 OIC provided by their institution.

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

FE and HE institutions should:
- Consult the notification template for FE and HE institutions provided by the Information Commissioner for guidance on best notification practice
- Audit their institutional personal data processing activities on an annual basis to ensure that these match the activities that have been notified

5.2 Processing Outside an Institutional Notification

Where employees process personal data for which the institution is not Data Controller such processing may 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 OIC by the individual

In neither case is the institution obliged to notify the OIC of the processing, or to ensure that the data protection principles are adhered to.

FE and HE institutions are not responsible for notification of personal data processed by employees for which the institution is not Data Controller e.g. for their own personal or domestic purposes.

FE and HE institutions are not responsible for ensuring that employees process personal data in accordance with the Data Protection Principles where the institution is not the Data Controller.

FE and HE institutions should ensure that employees are aware of the boundary between those personal data processing operations for which the institution is Data Controller, and those for which it is not.

FE and HE institutions might wish to consider, as part of their general institutional consciousness-raising exercises, providing employees 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.

5.3 Employee Access to, and Use of, Personal Data

Employees will often be expected to collect, hold, and process personal data for which their employer is Data Controller 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 are processing sensitive personal data in the course of their employment for which their employer is Data Controller.

FE and HE institutions should ensure that employees are:
- Aware that all personal data collected, held, and processed, on computer and on-line, are subject to the Data Protection Principles
- Aware that all personal data collected, held, and processed in structured manual files are subject to the Data Protection Principles
- Aware of the circumstances under which they may legitimately access, process and disclose personal data for which their employer is Data Controller in the course of their employment
FE and HE institutions should ensure that:

- All employee processing of personal data for which the institution is Data Controller must be for a purpose that is explicit, lawful and covered by the institution’s notification.
- For all employee processing of personal data for which the institution is Data Controller, whether on-site or off-site, clear processes must exist by which any data subject access request can be auditably satisfied.
- Guidelines for the proper use of personal data for which the institution is Data Controller 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 of the institution, for which the institution is Data Controller, whether in structured manual files or computerised form, in circumstances where data subjects feel that such use may cause them significant damage or distress.
6. Use of Personal Data by Students

6.1 Processing by Students where the Institution is the Data Controller

If an individual is acting as a student of the institution, and is processing personal data for which the institution is the Data Controller, then the institution is probably liable for any processing carried out by that student, meaning it is liable for compliance with all of the Data Protection Principles including, but not limited to, notification, as well as for provision of data in response to any subject access request.

In cases where students are processing personal data within FE and HE institutions for which the institution is Data Controller, the students conducting the research, or engaged in the course of study, can rely upon the notification to the OIC provided by their institutions.

FE and HE institutions should ensure that personal data for which the institution is Data Controller, and which is processed by students for research and study purposes is adequately covered by their institutional notification.

FE and HE institutions should ensure that where a student is processing personal data for which the institution is the Data Controller, all of the Data Protection Principles are complied with, and that information required for subject access requests can be supplied in a timely manner.

6.2 Processing by Students where the Institution is not the Data Controller

In cases where students are processing personal data within FE and HE institutions and the institution is not the Data Controller, the processing will be exempt from notification by the institution, and the institution will not be responsible for ensuring that it is carried out in accordance with the Data Protection Principles.

FE and HE institutions are not responsible for notification of personal data processed by students where the institution is not the Data Controller e.g. for students’ own personal or domestic purposes.

FE and HE institutions should ensure that students are aware of the boundary between those personal data processing operations for which the institution is Data Controller, and those for which it is not.

FE and HE institutions might wish to consider as part of their general institutional consciousness-raising exercises providing students 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.

6.3 Student Access to, and Use of, Personal Data

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 of their own, 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, including via websites and other Internet software are subject to the Data Protection Principles
- Aware that all personal data collected, held, and processed in structured manual files are subject to the Data Protection Principles
- Aware of the circumstances under which they may legitimately access, process and disclose personal
data for which the institution is Data Controller

FE and HE institutions should ensure that:

- There is clear, mandatory, process for prior formal authorisation and registration within the institution of such student processing
- Guidelines for the proper use of personal data are available to all students
- There is a mechanism to ensure that misuse of personal data for which the institution is Data Controller by students can be identified and remedied
- There is a mechanism for data subjects to object to the accessing, processing and disclosure of their personal data by students for which the institution is Data Controller, in structured manual files or computerised form, where data subjects feel it may cause them significant damage or distress
7. Data Sharing

7.1 General

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

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.

It should be noted that while transfers will be permitted where data subjects have given their consent to the transfer; consent cannot be inferred from silence, thus if the institution requests that consent be given by the data subject, in order that the institution can provide personal data to a third party, and no communication from the data subject is forthcoming, the institution must infer that consent is withheld.

Data may be disclosed to third parties in those circumstances where the DPA 1998 expressly permits transfers without such consent, for example where it is required for the:

- Purpose of protecting the vital interests of the data subject (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
- Purpose of preventing serious harm to a third party that would occur if the data were not disclosed
- Purpose of safeguarding national security
- Prevention or detection of crime
- Apprehension or prosecution of offenders
- Assessment or collection of any tax or duty or of any imposition of a similar nature
• Discharge of regulatory functions, including securing the health, safety and welfare of persons at work

With regard to the final 4 categories, it should be noted that disclosure is allowed in those cases only to the extent to which failure to disclose would be likely to prejudice the attainment of those aims. This may be difficult to ascertain by the Data Controller. However, most bodies that may request personal data in such circumstances should be able to provide documentary evidence to support their request. The absence of such documentation or a warrant may justify refusal to disclose the requested personal data.

See further ICO, Framework Code of Practice for sharing personal information [01/10/07]

7.2 Intra-Institutional 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.”

7.3 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 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?

The institution must ensure that personal data under its control is not disclosed or transferred to unauthorised third parties. Unauthorised third parties will include a person or organisation:

- Not covered by the data processing conditions relied upon by the institution under Sch.2 or Sch.2/Sch.3, unless the DPA 1998 expressly permits such disclosure or transfer – [breach of First Principle - lawful processing]
- Who is covered by the data processing conditions relied upon by the institution under Sch.2 or Sch.2/Sch.3, but where the request is for reasons outside the scope of those conditions, unless the DPA 1998 expressly permits such transfers without such consent. – [breach of First Principle - lawful processing]
- Not disclosed to the data subject as a likely recipient or class of recipient of their data in the institution’s fair information notice, unless the DPA 1998 expressly permits such disclosure or transfer – [breach of First Principle - fair processing]

“Unauthorised third parties” may include family members, friends, local authorities, and government bodies unless disclosure is permitted under the DPA 1998, or required by other legislation.

7.4 Disclosure Under s.28 & s.29 DPA 1998: National Security, Crime and Taxation

Section 28 DPA 1998 is a primary exemption for national security purposes. Section 29, DPA 1998 is a primary exemption for “crime and taxation purposes” and covers the following issues:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty

The exemptions provided under s.28/29 exclude personal data required for those purposes from certain elements of the DPA 1998, and permit the lawful disclosure of personal data to authorised bodies, such as the police, and other organisations that can rely upon this exemption because they have a crime prevention or law enforcement function e.g. the Benefit Fraud Sections of the Department for Work and Pensions or Local Authorities. They do not however require that disclosure be made – there is no general legal requirement under s.28/29 DPA 1998 to disclose information to the police or other authorised bodies.

Additionally, the disclosure exemption only applies where there is likely prejudice to one of the crime and taxation purposes. ‘Likely to prejudice’ means that to not disclose the information would noticeably damage those purposes. The ICO has advised that for the exemptions to apply there would have to be a substantial chance (rather than a mere risk) that in a particular case the purpose would be noticeably damaged. Thus, institutions will be required to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each individual case. This “prejudice” test must be applied unless an institution is under an express legal compulsion to disclose, for example where a court order has been served (see below).

Institutions should ensure that individuals claiming to be authorised to request personal data under s.28/29 DPA 1998 have their identity appropriately validated, and that the nature and scope of disclosure requested is necessary and proportionate to the aim to be achieved. The police and other authorised agencies often have standard forms which provide.
• Details about the individual requesting the information
• The individual’s organisational authorisation to make that request
• The case for disclosure

Institutions receiving a disclosure request, and who decide to disclose information are strongly recommended to keep a copy of all documentation, together with a record of the process by which the organisation reached the decision to disclose. These will be needed as evidence if an institution is subsequently challenged over its decision to disclose.


7.5 Disclosure to Employees under Discrimination Legislation

Given the perceived information asymmetry between employers and employees in complaints about discrimination at work, there has been increasing use within the field of discrimination law of procedures designed to permit employees greater access to information they require to support their claims. This process usually takes the form of the employee sending their employer a questionnaire requesting information relevant to their case. Such procedures exist under the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, and the Equal Pay Act 1970. In some cases the information which is sought will be personal data relating to other employees in the institution, who the complainant wishes to use as ‘comparators’ against which to contrast their own circumstances. Under the Equal Pay Act 1970, for example, the questionnaire is designed to enable an employee to get details about the pay and benefits package of the comparator(s) where they think that there is discrimination. Employers are not under a statutory obligation to provide answers to the questionnaire but an employment tribunal will be entitled to draw inferences from a deliberate refusal to answer or from an evasive or equivocal reply. The nature of the disclosures required by the employer, particularly under the EPA 1970, will raise data protection issues, for example where details of personal performance and appraisals, which the comparator employees may regard as their personal data under the DPA 1998, may be sought. Indeed, the questionnaire states that “certain information about individuals is protected by the common law of confidence and the Data Protection Act 1998”. The guidance notes that accompany the questionnaire go on to say “Where information is confidential, an employer would only be able to disclose the information if he had the consent of the individual in question, where he had a legal obligation to do so, or where there was a strong public interest requirement”.

This leaves the employer with a limited number of options:

• If proceedings have been started before the Employment Tribunal, then the employer may be able to rely upon s.35(2) DPA 1998, which permits disclosure of information for the purpose of legal proceedings, including prospective proceedings, or where disclosure is “necessary for the purposes of...defending legal rights”. However, this does not solve the confidentiality issues, or necessarily cover circumstances where an employee has merely served a questionnaire, without issuing a claim, as it is not clear whether this amounts to “prospective proceedings”. There is no compulsion to respond to the questionnaire; although an adverse inference can be drawn if an evasive, or no, response is given.

• In the absence of Tribunal proceedings, the employer may seek to reply upon the fact that disclosure is necessary for “the purposes of legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, except where the processing is unwarranted by reason of prejudice to the rights, freedoms or interests of the data subject.” There are clearly legitimate interests in play in as much the employer wishes to answer the questionnaire to avoid adverse inferences being drawn and the complainant wishes to have adequate information to pursue the Equal Pay claim. However, where information about a
comparator data subject’s pay and benefits or details of personal performance and appraisals is requested, the data subject may feel that their ‘rights, freedoms or interests’ are threatened. The ICO’s own Employment Code of Practice states that “Unless you are under a legal obligation to do so, only disclose information about a worker where you conclude that in all the circumstances it is fair to do so. Bear in mind that the duty of fairness is owed primarily to the worker. Where possible, take account of the worker’s views. Only disclose confidential information if the worker has clearly agreed”

- The employer may thus seek consent from the comparator data subject(s) to disclose the information, but where the material requested is considered by a data subject to be confidential or highly personal, this may well be refused
- The employer could provide aggregated information if more than one comparator is provided by the complainant or, where there is only one comparator, provide generalised information covering “details of pay schemes, job grading systems and job descriptions or how skills and experience are reflected in the employer’s pay system”. This could avoid both data protection and confidence issues, but might expose the employer to claims of evasiveness
- If consent is refused, and the employer does not wish to be seen to breach the DPA 1998, or confidentiality, they may withhold certain comparator data – if the Tribunal feels it necessary, it has the power to require disclosure. At this point the employer cannot be held liable for disclosure, but may already have damaged its position before the Tribunal. It is advisable therefore to make it clear to the Tribunal that in withholding the information the employer is maintaining its responsibilities to its comparator data subjects, and not objecting to the disclosure itself

7.6 Mandatory Disclosures

While the DPA 1998 itself does not oblige institutions to disclose personal data to specific third parties, personal data are exempted from the non-disclosure provisions where the disclosure is required by legislation, 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 their staff and students are properly warned of any known statutory disclosures that the institution is 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 Table 2.

7.7 Verification of Student Attendance and Qualifications

Employment agencies and prospective employers often contact institutions to verify details about a student, such as attendance records, examination results, and degree classifications. In most circumstances, students would not object to the disclosure of such information, and indeed disclosure would appear to benefit the student.

Such a request for information should be treated as an FOI request. This will require an institution to consider whether the request should be refused by virtue of s.40 FOIA/s.38 FOISA. Under those sections, personal data is exempted from disclosure if that disclosure would any breach any of the data protection principles; or s.10 DPA 1998 (the data subject’s right to prevent processing likely to cause damage or distress). Where the personal data does not contain sensitive data and the institution:

- Believes that disclosure is necessary for the purposes of legitimate interests pursued by the third party, and has no reason to believe that the disclosure would prejudice the rights and freedoms or legitimate interests of the data subject (such as a s. 10 DPA 1998 notification by the data subject) and
- Has included employment agencies and prospective employers in its fair information notice
Reports to Parents and Sponsors

It is common practice for institutions to require students below the age of 18 to consent to sending of routine reports on academic progress and attendance to their parents as part of their application and enrolment practice. However, other non-routine requests for information from parents or carers should be considered carefully, and it is usually the case that permission will be requested from the student before disclosing any additional information.

Many students attend college under sponsorship agreements, e.g. with employers. This may include paid time to attend or payment of fees. It is common practice for institutions to require students to consent to the sending of routine reports to their sponsors on academic progress and attendance as part of their application and enrolment practice. In the absence of student consent allowing the institution to disclose, or their having agreed with their sponsor that such reports may be made, it may be the case that where the institution:

- Believes that disclosure is necessary for the purposes of legitimate interests pursued by the sponsor, and has no reason to believe that the disclosure to the requester would be permissible, even without the consent of the data subject. However, it is worth remembering that for disclosure in this case to meet the fair and lawful processing requirements of the DPA1998, that a Sch.2 condition must be demonstrated. This will require some thought about effective verification of the requester’s legitimate interests in obtaining the personal data.

In circumstances where the institution:

- Has already fairly and lawfully publicly disclosed the information requested e.g. by publication of examination results by candidate name in the media
- There has been no intervening s.10 DPA 1998 notification by the data subject

it would appear difficult to argue that disclosure under FOI could be plausibly exempted under s.40 FOIA/s.38 FOISA.

7.8 Reports to Parents and Sponsors

It is common practice for institutions to require students below the age of 18 to consent to sending of routine reports on academic progress and attendance to their parents as part of their application and enrolment practice. However, other non-routine requests for information from parents or carers should be considered carefully, and it is usually the case that permission will be requested from the student before disclosing any additional information.

Many students attend college under sponsorship agreements, e.g. with employers. This may include paid time to attend or payment of fees. It is common practice for institutions to require students to consent to the sending of routine reports to their sponsors on academic progress and attendance as part of their application and enrolment practice. In the absence of student consent allowing the institution to disclose, or their having agreed with their sponsor that such reports may be made, it may be the case that where the institution:

- Believes that disclosure is necessary for the purposes of legitimate interests pursued by the sponsor, and has no reason to believe that the
<table>
<thead>
<tr>
<th>Third Party</th>
<th>Authorisation for disclosure</th>
<th>Further Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors.</td>
<td>Further and Higher Education Act, 1992 s.79</td>
<td>The Funding Councils are able to request such information as they may require for the purposes of the exercise of any of their functions under the Education Acts</td>
</tr>
<tr>
<td>Connexions Service</td>
<td>Learning and Skills Act 2000</td>
<td>The Connexions Service may request the names and addresses of students between ages 13 to 19 and/or their parents</td>
</tr>
<tr>
<td>Electoral registration officers</td>
<td>Representation of the People Act 2000; The Representation of the People [England and Wales] Regulations 2001</td>
<td>Electoral registration officers may request information required for the purpose of voter registration</td>
</tr>
<tr>
<td>Officers of the Department of Works and Pensions, and Local Authorities</td>
<td>Social Security Administration Act 1992: s.110A, s.109B and s. 109C</td>
<td>Designated Officers can request information and documents or copies of, or copies of extracts from, such documents as they may reasonably require for the purpose of investigation of benefit fraud</td>
</tr>
<tr>
<td>Health and Safety Executive</td>
<td>Reporting of Injuries, Diseases and Dangerous Occurrences Regulations [RIDDOR] 1995 s.3</td>
<td>Required for the purpose of notification and reporting of injuries and dangerous occurrences</td>
</tr>
<tr>
<td>Audit Commission and related auditing bodies</td>
<td>Audit Commission Act 1998 s.6</td>
<td>An auditor has a right of access at all reasonable times to every document relating to a body subject to audit which is necessary for the purposes of their functions under this Act</td>
</tr>
<tr>
<td>Environmental Health Officers</td>
<td>Public Health [Control of Disease] Act 1984 and the Public Health [Infectious Diseases] Regulations 1988</td>
<td>EHOs have powers to obtain information for the purpose of reporting notifiable diseases</td>
</tr>
<tr>
<td>Child Support Agency</td>
<td>Child Support [Information, Evidence and Disclosure] Regulations 1992.</td>
<td>The Child Support Agency has powers to obtain certain information from, amongst others, the relevant parties, employers and local authorities.</td>
</tr>
<tr>
<td>Inland Revenue</td>
<td>Taxes Management Act 1970.</td>
<td>HMRC can require organisations to supply them with information about various categories of people.</td>
</tr>
<tr>
<td>Police Officers</td>
<td>With a Court Order.</td>
<td>Disclosures to the Police are compulsory in cases where the institution is served with a court order requiring personal data.</td>
</tr>
<tr>
<td>Other third parties</td>
<td>With a Court Order.</td>
<td>Disclosures to third parties are compulsory in cases where the institution is served with a court order requiring personal data.</td>
</tr>
</tbody>
</table>
Disclosure to the Border and Immigration Agency (BIA)

The Border and Immigration Agency does not currently have a legal right to make blanket requests for information about students, but is entitled to ask for information about specific students. For example, an immigration official may want to confirm the dates a student is studying at the University if they have entered the UK on a short-term visa.

It is good practice only to disclose student information after the following criteria have been met:

- Reasonable efforts have been made to ensure the enquiry is from a bona fide immigration official, e.g. the request should be made in writing on official paper and the relevant exemption is quoted
- It is a genuine enquiry about a specific, named student

Other Disclosure Issues

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

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

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

Provision of Guidance

It is helpful for institutions to provide clear guidance to their staff on good practice in disclosure. Provision of such guidance helps to ensure a consistent and coherent institutional approach, and cross-institutional adherence to it will also encourage good practice on the part of information requestors in their dealings with the institution.

Examples include:

University of Brighton, Guidelines for disclosure of student personal data [March 2008]

University of Edinburgh, Guidelines on disclosure of information about students [Jan 2008]
http://www.recordsmanagement.ed.ac.uk/InfoStaff/DPstaff/DP Students/DisclosureOfStudentInfoV8.htm

FE and HE institutions should ensure that:

- Their staff and students are aware that, as data controllers, institutions owe an obligation to data subjects not to pass on their personal data to third parties, unless this is covered by the data processing condition relied upon by the institution under Sch.2 or Sch.2/Sch.3, or the DPA 1998 expressly permits such disclosure or transfer
- Their staff and students are aware that third party requests for personal data held by the institution should be properly treated as FOI requests, and that refusal to supply personal data will have to be justified by reference to s.40 FOIA/s.38 FOISA
- At the time that their personal data is collected, data subjects are informed about the purpose of the processing and the recipients (or classes of recipients) to which that information will, or may be, disclosed. Ideally, where it is not unduly onerous for the institution to do so, they could provide the reason or reasons for the disclosure to the third party, in the interests of fairness and transparency
- Where an employee requests personal data about another data subject within the institution, such
information should be released only if, and only to
the extent that, the member of staff requires the
information in order to perform his or her official
duties, or is permitted by law to make such a
request
• The legal restrictions upon an institution’s ability
to disclose personal data to third parties are
communicated clearly to parents, relatives and
guardians of staff and students when requests for
personal data are made. It is widely recognised
as bad practice for institutions and their
employees simply to announce that “The Data
Protection Act won’t let us do that”
• Reasonable measures are in place to prevent the
inadvertent disclosure of personal data (i.e. a
student’s current attendance at a particular
institution) to unauthorised third parties. When
staff receive requests as to whether a named
person is currently a student of the institution,
unless the request falls outside the s.40 FOIA/38
FOISA personal data exemption, the member of
staff should decline to comment one way or the
other
• Enquiries from Embassies and High Commissions
are treated with extreme caution. Data subjects
may choose to have little or no contact with
representatives of their home states, the extent of
the relationship is a matter for the data subject,
not the institution, to determine
• If a request for information about a data subject is
refused, but the subject-matter of the enquiry is
evidently of importance to the data subject, they
should be informed of the enquiry. This will allow
the data subject to contact the enquirer should
they so wish

FE and HE institutions may wish to consider advising
staff that:
• Where a request for information is received by
telephone from an enquirer who appears to be a
person to whom information may properly be
disclosed, it is good practice to offer to telephone
back with the information to ensure some
measure of authentication
• As an alternative to divulging personal data, an
institution will be willing to accept a sealed
envelope which it will attempt to forward to the
student’s last-recorded address or to forward an
incoming email message to a student
• Where the matter is urgent, an attempt should be
made to contact the student by telephone, or other
means, in order to provide them with information
about the enquirer and the nature of the enquiry,
so that they can choose whether to respond

When dealing with third parties claiming the right to
access to a data subject’s personal data under any of the
DPA 1998 exemptions described above, or mandatory
provisions in other legislation, FE and HE institutions
should, except in emergency situations:
• Require such requests be directed to a specific set
of people authorised to decide whether or not to
release personal information under the exemption
• Only disclose personal data in response to an
adequate and properly authorised written request, including
  o details of the authority under which the request
    is made
  o reasonable proof of the requester’s personal
    identity and organisational affiliation
  o the nature of the personal data requested and
    the purpose for which it is being requested; and
  o a warrant that it will be held and processed in
    conformity with the Data Protection Principles
• Make a record of each decision made and the
reasons for that particular decision

An emergency situation is one where there is reason
to believe that there is a danger of death or injury to
the data subject or any other person. In emergency
situations, staff should be advised:
• If possible, to seek the authorisation of a senior
manager before disclosure
• Not to disclose data where they have doubts
  as to the validity of the request
• Where the request is received by telephone, to ask
  the caller to provide a switchboard number, and
call them back through the organisation’s
switchboard before providing the data
• To keep a record of the enquiry and their
  response, and pass this to the institution’s Data
Protection Officer as soon as possible
• To ask the enquirer to follow up their request with
  a formal written request, so the institution has a
record on file
8. Security of Personal Data

8.1 Institutional Framework for Data Security

A data subject may apply to the court for compensation if they have 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 Controller, or access has been obtained to personal data without the authority of the Data Controller. 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.

FE and HE institutions are obliged under the DPA 1998 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 ISO27002 (previously BS7799). A framework that meets this standard will provide a high level of compliance with the DPA 1998. Where complete compliance with ISO27002 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

FE and HE institutions should consider the:

- Extent to which their personal data holdings are computerised or manual, and whether existing computerised and manual systems duplicate certain types of personal data
- Extent to which their personal data holdings are distributed around their site(s), and how this distribution affects the management and security of such holdings, particularly of manual holdings

- Appropriateness of manual storage of personal data, with the difficulties of ensuring viable backup, security, and management systems in paper or microfiche holdings
- Desirability and feasibility of computerised systems where data are de-personalized, or coded, or encrypted, with a secure key

FE and HE institutions should ensure that:

- Reasonable access control mechanisms including, where appropriate, the use of passwords, encryption, compartmentalised access and access logs, are used to detect and prevent attempts to access computer files through terminals or computer networks without authorisation
- Reasonable access control mechanisms including, where appropriate, security locks, secure rooms, authorised key holders, and access logs are used to monitor access to manual files to prevent unauthorised access
- 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

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

- Existing and proposed personal data processing operations are evaluated for potential risks in order to determine the cost, effectiveness and practicability of proposed levels of security
- Appropriate levels of security are applied, commensurate with the anticipated risks, and appropriate to the type of personal data held
- Agreed levels of security are applied, monitored and regularly reported upon as regards their effectiveness
• All staff are trained to take effective action to protect personal safety, data and equipment (in that order) in the event of disaster
• Competent people are assigned to be responsible for the accuracy and integrity of personal data held in each part of an institution’s personal data processing operations

8.2 Employee Security Training and Management

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

FE and HE institutions should ensure that:

• Employees dealing with personal data, for which the institution is Data Controller, 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 dealing with personal data, for which the institution is Data Controller, 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 dealing with personal data, for which the institution is Data Controller, 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 for unauthorised purposes (e.g. browsing of personal data, whether on computer or in manual files) will be a disciplinary offence
• Employees must apply and abide by any relevant security requirements contained in agreements with outside bodies who may furnish personal data for university research purposes.
• Employees are aware that casual access to personal data, for which the institution is Data Controller, by unauthorised persons (e.g. members of the general public having access to personal data via VDU screens or printouts, or in unlocked filing cabinets stored in corridors or in unlocked rooms), by act or omission, should not be permitted. Institutional regulations should provide that acts or omission that do, or could lead to unauthorised access or disclosure to unauthorised persons will be a disciplinary offence
• Institutional regulations provide that failure to adhere to the correct use of applicable access control mechanisms will be a disciplinary offence

8.3 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.

FE and HE 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

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

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

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

8.4 Students

It is not envisaged that many students will have access to or be processing personal data for which their educational institution is the Data Controller. This is particularly so for undergraduate students. However, students in certain subjects, such as medicine and certain social sciences, may be permitted to access or process personal data for which their educational institution, or a partner of their educational institution, is the Data Controller, in the courses of their studies or research.

It is recommended that FE and HE institutions should ensure:

• That processing of personal data for which the institution is the Data Controller, by students as students, if allowed, is not allowed off-site, but it is recognised that, particularly with postgraduate research students, this may not in fact always be practical. In such circumstances, research students should be given formal training in their own and their institution’s obligations under the DPA1998, and advised on appropriate security measures. This could be carried out as part of an institution’s ethical review process for postgraduate research projects.

FE and HE institutions should ensure that:

• Students dealing with personal data, for which the institution is Data Controller, 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.

• Students dealing with personal data, for which the institution is Data Controller, 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).

• Students dealing with personal data, for which the institution is Data Controller, are aware that their access to personal data is for specified authorised purposes only. Institutional regulations should provide that access to personal data by students for unauthorised purposes (e.g. browsing of personal data, whether on computer or in manual files) will be a disciplinary offence.

• Students must apply and abide by any relevant security requirements contained in agreements with outside bodies who may furnish personal data for university research purposes.

• Students are aware that casual access to personal data, for which the institution is Data Controller, by unauthorised persons by act or omission, should not be permitted. Institutional regulations should provide that acts or omission that do or could lead to unauthorised access or disclosure to unauthorised persons will be a disciplinary offence.

• Institutional regulations provide that failure to adhere to the correct use of applicable access control mechanisms will be a disciplinary offence.

8.5 Transfer of Personal Data

Reasonable precautions must be taken when transferring personal data in either hardcopy or electronic form. Institutions should be aware of the data transfers being undertaken by employees and students for which the institution is the Data Controller. Rules ensuring an appropriate level of authorisation for particular transfers, especially data transfers containing sensitive personal data, or data the inadvertent disclosure of which is likely to cause distress or damage to data subjects e.g. financial information, should be embedded in an institution’s administrative policies.

FE and HE institutions should not assume that documents transferred by electronic means (e.g. e-mail, web transfers, FTP) are secure. Material containing
sensitive personal data, or data the inadvertent disclosure of which is likely to cause distress or damage to data subjects, e.g. financial information, should always be encrypted to an appropriate standard before transfer, as should information sent by post or courier on CDs, DVDs and data sticks. Personal data sent in hardcopy form should also be transferred in a manner appropriate to its sensitivity.

FE and HE institutions should ensure that:

• Transfers of personal data are authorised and/or conducted at an administrative or managerial level appropriate to the type of personal data to be transferred
• Personal data is transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of personal data to be transferred

8.6 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.

FE and HE institutions should ensure that:

• Future migration or upgrade plans for institutional systems are documented to address the potential effect of hardware, software and operating system upgrades, or obsolescence, on personal data processing operations
• Successful data transfer tests of existing personal data to new systems or file formats are carried out before those systems go live, and old systems, including manual systems, are discarded

8.7 Back-up of Personal Data

Loss or destruction of personal data may have severe consequences for the operations of FE and HE 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.

FE and HE institutions should ensure that:

• A workable and documented 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
• Decisions whether or not to implement a disaster recovery mechanism for any particular personal data processing operation are justified and documented
• 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, taking into account the nature and importance of the personal data

8.8 Processing of Personal Data Off-site, on Home Computers, or at Remote Sites

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

Employees and students should take particular care when laptop computers or personal machines are used to process institutional personal data at home or in other locations (e.g. in public places, or on public transport) outside the institution. Laptops containing personal data should have properly implemented security measures that are proportionate to the anticipated risks and appropriate to the type of personal data to be transferred. These may include passwords, biometric security mechanisms and encryption.
36

The increasing capacity and declining size of storage media, such as CDs, mini hard disk drives, and USB flash memory data sticks means that it is possible for employees and students to carry considerable amounts of personal data on media that are easily lost or forgotten. Institutions should consider the provision of advice to employees and students about the appropriate use of such media and the need for adequate security measures to reduce data breaches in the event of loss or theft.

Employees and students should be required to ensure that when processing personal data for which the institution is Data Controller at home or in other locations:

- They take reasonable precautions to ensure that the data is not accessed, disclosed or destroyed as a result of act or omission on their part
- They ensure personal data held in manual form is stored as securely as possible, and ideally is locked away when not in use
- They have an up-to-date firewall and a virus-scanning program installed on laptop computers or personal machines and scan all disks, e-mails, and other potential virus vectors for viruses
- They back-up system hard drives to avoid loss of data
- They report all computer security incidents including virus infections to the institution

Employees and students should be required to ensure that when using laptops to process personal data for which the institution is Data Controller they:

- Keep the laptop constantly in view when travelling, especially in busy places/terminals such as airports
- Do not check the laptop as baggage unless it is placed inside luggage that has been locked
- Record the model number and serial number of each hardware component associated with the laptop and keep this information in a separate location
- Notify the institution immediately in the event of loss or theft of personal data on any laptop, PDA, or other digital storage mechanism or media

8.9 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 proportionate to the anticipated risks and appropriate for the type of 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 either be overwritten to a suitable standard or destroyed.

FE and HE 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, where appropriate, students are provided with guidance as to the correct mechanisms for disposal of different types of personal data and regular audits should be carried out to ensure that this guidance is adhered to. In particular, employees and students should be made aware that erasing electronic files does not equate to destroying them

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

9.1 Examination and Assessment Process

The DPA 1998 provides exemptions that apply to some parts of the examinations process. However, these exemptions are limited in scope, and some are time-limited, e.g. the exemption is for a limited period of time.

FE and HE institutions should assume that, with the exception of those parts of the examination process that are specifically exempted by the DPA 1998, 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.

9.2 Examination Scripts

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

FE and HE institutions have the absolute discretion to deny subject access requests for examination scripts. However, the fact that the exemption is discretionary means that an institution may still choose to provide examination scripts under a subject access request.

9.3 Examiners’ Comments

Both internal and external 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 DPA 1998. 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.

Providing feedback “in intelligible form” may require institutions to consider the form in which examiner’s comments are produced. If comments are written directly onto scripts, their nature may mean that they can only be produced “in intelligible form” in relation to a particular part of the script (e.g. “this section is very poor”). Requesting that examiners write comments in a form that are readily comprehensible even in the absence of the script will reduce the likelihood that the institution finds itself only able to meet this requirement by producing the script.

Provision of feedback on both formative and summative assessment is increasingly seen as an important part of the educational process -

QAAHE Code of Practice on Assessment, Precept 12:

“...Institutions should ensure that appropriate feedback is provided to students on assessed work in a way that promotes learning and facilitates improvement.”

It is increasingly likely that institutions will be aiming to provide feedback to students within an appropriate timescale for students’ educational development. In such circumstances the need for a student to make a subject access request for personal data such as examiners’ comments will be significantly reduced.

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

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

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

The DPA 1998 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. FE and HE 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, FE and HE institutions usually already provide such explanation, as a review of administrative procedures will normally be required in the event of a student appeal against classification etc.

FE and HE 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

9.5 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. This is unlikely to be onerous if the identity of the third party can be easily withheld by erasure from the disclosed material. Note that this is subject to the proviso that the third party may consent to the disclosure, or the disclosure may be "reasonable in all the circumstances." However, obtaining the consent of the third party in such circumstances may be difficult/impossible, and rather than making an institutional judgment on what "reasonable in all the circumstances" means in such circumstances, it may be sensible to let the data subject ask the OIC to make that determination, if necessary.

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. This is unlikely to be onerous if the identity of the third party can be easily withheld by erasure from the disclosed material. Note that this is subject to the proviso that the third party may consent to the disclosure, or the disclosure may be "reasonable in all the circumstances." However, obtaining the consent of the third party in such circumstances may be difficult/impossible, and rather than making an institutional judgment on what "reasonable in all the circumstances" means in such circumstances, it may be sensible to let the data subject ask the ICO to make that determination, if necessary.

It should be noted that examination board minutes and related documentation that concerns general discussions, e.g. about moderation standards, will very likely be accessible to individuals under FOI legislation, unless an exemption can be claimed.

FE and HE 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
9.6 Disclosure of Results

As personal data, examination results should not be disclosed to third parties unless one of the criteria in Schedule 2 DPA 1998 is met. This does provide FE and HE 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. It is possible in such circumstances for an institution, rather than seeking consent for the publication of results, to rely on the “legitimate interests” condition, whilst giving students an opportunity to opt out. If a student opts out of publication, the institution should then not disclose results to enquirers, unless requested by the data subject, or where there is legitimate reason to do so, such as the prevention of fraud, e.g. where a student misrepresents their results to an employer.

FE and HE 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

FE and HE 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

FE and HE institutions should consider:

- A mechanism for data subjects to indicate their wish to opt out of the institution displaying their results in particular fora
- Publishing results on publicly accessible notice boards with PINs instead of names
- Providing results to students face-to-face, via post, or via secure electronic means
10. Use of Personal Data in Research

10.1 General

The DPA 1998 provides exemptions for ‘research purposes’ including statistical or historical purposes. Where processing for research purposes is not used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, it is exempt from:

- The Second Principle - personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes - personal data can be processed for research purposes other than for which they were originally obtained
- The Fifth Principle - personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes – personal data processed for research purposes can effectively be held indefinitely

Additionally, where:

- Personal data is not processed to support measures or decisions with respect to particular individuals
- Personal data is not processed in a way that substantial damage or distress is likely to be caused to any individual
- The research results, or any resulting statistics, are effectively anonymised

there is an exemption from the data subject’s right of access. The data controller may still choose to disclose the information to the data subject, unless by doing so they would breach another individual’s data protection rights.

In addition to the legitimate purposes for processing of sensitive personal data contained in the DPA 1998 (e.g. explicit consent, medical research by a health professional), the Data Protection [Processing of Sensitive Personal Data] Order 2000 expressly permits processing for research purposes ‘in the substantial public interest’ where the 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.

While some exemptions are granted for use of personal data for research purposes; there is no blanket exemption from the Data Protection Principles. Thus:

- Research data subjects should be informed of any new data processing purposes, the identity of the Data Controller, and any disclosures that may be made
- Research data subjects must be able to meaningfully exercise their right to object to the data processing because it would cause/has caused, them significant damage or distress
- Requirements for appropriate security of data must be respected, including appropriate levels of security for sensitive data
- Data may not be transferred to researchers in a non-EEA country, unless that country has adequate data privacy protections, the data subject’s explicit consent has been obtained, or there is an appropriate data protection contract with the data recipient

The legislation recognises that the value of access to personal data in research may outweigh a data subject’s desire to exercise a high level of control over the use of their data. As a result, even researchers wishing to use sensitive personal data should be able to do so, if they can demonstrate a significant public interest, and they adhere to the procedural safeguards required by law.

FE and HE institutions should ensure that:

- Employees and students are aware that, while some exemptions are granted for the use of personal data for research purposes, the majority of the Data Protection Principles must still be conformed to – there is no blanket exemption
- In all circumstances where personal data is to be used for research purposes, that data protection issues are adequately addressed in institutional ethical research review processes, in advance of processing, to ensure that the requirements of the DPA 1998 will be adhered to
• Data protection procedures and practices in research areas are monitored periodically to ensure adequate compliance
• A suitable mechanism is in place to ensure that data subjects whose personal data is to be, or has been, processed can meaningfully exercise their right to object to the processing of that data on the grounds that it would cause them, or has caused them, significant damage or distress
• Particular care is taken when the processing involves sensitive personal data

FE and HE institutions are advised always to provide as clear guidance as possible to data subjects, whose personal data will be used in research, as to why the data is being collected and the purposes for which it will be used.

10.2 Online Research with Human Subjects

For many on-line research projects, existing ethical guidelines on issues such as informed consent, ability to withdraw, and data security, will already meet the requirements of data protection law. Most guidelines assume that online researchers will request informed consent from respondents in advance of conducting research, and will provide means for respondents to withdraw that consent. Where this is not the case researchers will have to justify their actions under ethical guidelines, and also demonstrate that their data processing is fair and lawful under the DPA 1998.

However, researchers seeking to gather research data online should be aware that the online environment generates significant amounts of ‘background information’ – data logs, IP address collection, cookies, caches, etc. This information is often ‘sticky’ - it is difficult to entirely disassociate it from the ‘foreground information’ that the researchers are interested in. Equally, use of Internet research tools and computer systems will require researchers to identify and address potential technical and administrative problems, e.g. poor research tool configuration and inappropriate levels of system security/integrity.

FE and HE institutions should ensure that:
• Employees and students are made aware of the particular data privacy risks of conducting research with human subjects using online research tools
• Suitable training is provided to employees and students to ensure that they are aware of any technical requirements or hardware or software configuration issues that should be considered in order to provide appropriate security for the type of personal data processed
• Ethics review processes involve staff who can adequately assess the data protection risks arising from the use of online research tools, and the adequacy of the solutions proposed to address them

10.3 Provision of Research Data to 3rd Parties

By early 2008 there has still been little judicial consideration of the issue of data protection and the provision of research data to third parties. One case, Common Services Agency v Scottish Information Commissioner (2006), has, however, dealt with the issue of the provision of research data held by a “public authority” to a 3rd party under the FOISA 2002.

In the Common Services Agency case, the applicant requested data on incidence of childhood leukaemia in Dumfries and Galloway from the NHS statistical service, the Common Services Agency (CSA), under the FOISA 2002. The CSA declined to provide data on the grounds that the number of cases was very small and there was a risk of identification of living individuals, thus the data was exempt information under FOISA. The applicant appealed to the Information Commissioner, who ruled that the Agency should supply the information to C in a “barnardised” form, a system by which small numbers are randomly either left unmodified or modified by adding or subtracting one so as to minimise the risk of identifying individuals. The CSA appealed that ruling. A number of important issues for researchers arise from that appeal. The court held that:
• A barnardised table setting out the census ward data for 1990-2001 for the Dumfries and Galloway postal area did not constitute personal data of any of the children resident in the area who had in a relevant year been diagnosed with leukaemia, as the information had not only become statistical but perturbed to minimise the risk of identification of any individual child. It was not “biographical in a significant sense”, as per Durant.

• Even though the CSA did not hold the relevant data in barnardised form at the time of the applicant’s request, the barnardised data was different from the raw data not in kind, but only in presentation. The CSA was not being asked to create new data by providing barnardised data, but was simply presenting underlying original data in a form that protected confidentiality.

• The CSA as a public authority was obliged to provide reasonable assistance and advice to the applicant with respect to his FOISA request. That obligation included providing an outline of different kinds of information which might meet the terms of the request. The relevant data and their disclosure in barnardised form could be required of the CSA in furtherance of that obligation, subject to any objection on ground of cost or to any fees chargeable. In this case the CSA could produce the barnardised data without undue difficulty.

The case is, however, under appeal in the House of Lords. Early indications from arguments before the House of Lords suggest that the court will determine that the barnardised data in question are in fact personal data. The case may provide some further guidance on the definitions of ‘personal data’ and ‘sensitive personal data’, as well as some indication of factors that public authorities should consider when identifying, assessing and balancing any legitimate interest of the public in disclosure as against the rights of the individuals affected against unwarranted privacy intrusion. A full decision is expected in late 2008.

As matters currently stand, prior to any decision in the CSA case, FE and HE institutions who receive FOIA requests for information by third parties for research data not exempted under other FOIA provisions, such as the ‘publication exemption’, should consider when deciding whether to release the data:

• Whether the data requested may contain personal data, i.e. living individuals can be identified from the data, or from the data in combination with other information likely to be available to the third party.
• Where there is a risk of identification of any data subject, whether that risk can be removed by:
  0 redaction of data
  0 provision of data in statistical form or
  0 provision of data in statistical form after barnardisation, or similar anonymising perturbation.
• Whether the cost of providing the data in appropriately anonymised form is reasonable on ground of cost.
11. References

11.1 References Given by FE and HE Institutions

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

- Education, training or employment of the data subject
- Appointment of the data subject to any office
- Provision by the data subject of any service

FE and HE institutions have the absolute discretion to refuse to release references written on their behalf if requested to do so in, or as part of, a subject access request. However, the fact that the exemption is discretionary means that an institution may still choose to provide references written on their behalf under a subject access request.

11.2 References Received by FE and HE Institutions

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

- The identity of the referee can be protected by anonymising the information
- This referee has given his/her consent
- It is reasonable in all the circumstances to release the information without consent

In considering whether it is reasonable in all the circumstances to comply with a request, the ICO suggests Data Controllers should take account of factors such as:

- Whether the referee was given express assurances of confidentiality
- Any relevant reasons the referee gives for withholding consent
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been advised of any weaknesses
- Any risk to the referee

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

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

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

FE and HE institutions should consider:

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

There may be circumstances where a reference is written on behalf of a data subject by an individual in one department of an FE or HE institution, to be used by an individual in the same institution or even the same department. While in principle, there is no obvious justification for differentiating between references received from external third parties, and references received from within the institution, as regards any consideration of data subject access, it appears from reported FE/HE experience that the ICO considers internal references to be ‘management data’ rather than references, and that disclosure may thus be required.

When dealing with subject access to a reference sent and received internally FE and HE institutions should treat that reference as management data and not as a reference.
12. The Internet and Online Services

12.1 Institutional Web Pages

Most, if not all, FE and HE institutions now have both a public Internet presence, in the form of a website containing a range of information about the institution and accessible world-wide; and an intranet, again usually web based, but only accessible to members of the particular institution. Within the set of web pages that make up both institutional Internet and intranet websites there will be web pages that contain personal data such as staff names, pictures, contact details etc.

Such data, when released on the public Internet, by definition goes beyond the EEA, including to countries that do not have data privacy regimes considered adequate by the EU Commission, and would thus appear to contravene the Eighth DP Principle. However, the ECJ, in the case of Lindqvist (2003), stated that “there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.” Despite this, it should be remembered that placing material on a web page is a very open form of publication, and data subjects should be able to exert their normal rights (as in DP Principle 6). Where FE and HE institutions use personal data in this way consideration needs to be given to the justifications for the display of the data, and whether these demonstrate that the use of the personal data in this fashion is both necessary and proportionate.

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

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

FE and HE institutions may use non-sensitive staff personal data on institutional Internet and intranet web pages 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 web pages, and have the right to object to the use of their data where it would cause them significant damage or distress. Retaining the right to object does not mean automatically being able to have data removed, rather that the data subject is in a position to make their objections known - the institution can then make a determination on whether the damage or distress alleged is a suitable ground for removal.

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

FE and HE institutions should not use sensitive staff or student personal data on institutional Internet or intranet web pages without explicit consent unless those web pages are only accessible to the data subject.
12.2 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 FE and HE institutions, need not require the consent of the data subjects, if restricted to use on an institutional intranet. However, data subjects whose personal data is used in this way should still retain the right to object to the use of their data where it would cause them significant damage or distress.

Where staff on-line telephone and e-mail directories are made available on the Internet, for the purposes of the normal organisational functioning and management of the institution, this need 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 it seems reasonable to expect that consent should be obtained from data subjects. Even where consent has been obtained institutions should have an easily accessible mechanism for the withdrawal of that consent allowing students to cease having their details displayed.

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

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

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

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

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

FE and HE institutions should obtain consent from student data subjects before including their personal data in on-line e-mail directories available on an institution’s Internet website. Student data subjects should be able to easily withdraw that consent and thus cease having their details displayed.

12.3 Web Pages Used to Collect Personal Data

Many FE and HE 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.

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

- The purpose for which the data is collected
- The recipients or classes of recipients to whom the data may be disclosed
- An indication of the period for which the data will
be kept (e.g. “while we process your application”, “for the duration of your studies” etc. rather than a specific time period.)

• And any other information that may be required to ensure that the processing is ‘fair’

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

FE and HE 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.

12.4 Personal Employee and Student Web Pages on Institutional Machines

In some institutions, employees and students have been permitted to create personal web pages on institutional servers, or even to run their own web servers. This policy approach has been justified on the grounds that use of such facilities serves an educational purpose.

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

FE and HE institutions should consider:

• Whether employees and students should be permitted to run personal web servers or to have personal web pages on institutional machines where such web servers and web pages are used for purposes unconnected with their employment or studies
• The terms and conditions under which such personal web servers or personal web pages should be permitted, if allowed

12.5 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 JANET (UK) to ensure as far as possible that their users do not use the SuperJANET system to transmit or transfer certain types of electronic data. They are obliged by law to report to the police the discovery of certain types of electronic data, if that data is found on their equipment, or transmitted across their networks.

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

• Network administrators’ using of log files for administrative purposes
• Email 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’ computer 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.

FE and HE 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.

FE and HE 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

FE and HE institutions should provide:

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

### 12.6 Web 2.0 Services

The use of Web 2.0 services (Facebook, Second Life, Bebo, blogs, Wikis and other externally hosted services) is a recent development in FE and HE service provision. It is important to understand that use of externally hosted services may carry data protection implications for institutions, their staff and their students. In most cases, it is quicker and simpler to avoid difficulties by addressing compliance issues when setting up a service, rather than waiting to deal with potential non-compliance issues when they arise.

When using externally-provided Web 2.0 services, it is almost always necessary to use personal data – for instance, the user’s email address, name, perhaps their address, personal interests etc – and in those cases the DPA 1998 will apply. If you enter into an arrangement with an external service provider for the provision of Web 2.0 services, it is necessary to consider the following data protection risks.

**The Role of the Service Provider** - Is the nature of the arrangement such that the institution will be legally responsible for any breaches of the DPA 1998 by the service provider? If the service provider is explicitly contracted to provide particular services for the institution in such a way that they become a data processor acting on behalf of the institution, then the institution will be responsible, as data controller, for ensuring that the service provider’s processing is in conformity with the Act. A service provider may be deemed to be acting as a data processor for an institution where:

- The institution has negotiated a specific agreement with the service provider
- The service is branded as an institutional service
- It is not immediately apparent to users of the service that they are providing data to an external service provider rather than to the institution
- Students must sign up to the service as a compulsory requirement of a course or programme
- The service provider can only use the data in ways or for purposes specified by the institution
When entering into relationships with Web 2.0 service providers where there appears to be a data controller/data processor relationship, institutions should ensure that there is a data processing contract between the service provider and the institution covering the relevant legal obligations.

Where possible, institutions may wish to avoid becoming legally responsible for Web 2.0 service providers’ compliance with the Data Protection Act by ensuring that it is clearly stated that service providers are separate legal entities, and that the institution is not determining the purposes for which, and the manner in which, any personal data are, or are to be, processed and is thus not a data controller for the data.

This can be supported by processes such as:

- Clearly identifying that the service is provided by an external service provider, both on the site itself, in any supporting institutional documentation (e.g. course handbooks) and in the way that the user access the service (e.g. if students enter the site from WebCT, that they are given a message that they are now leaving the institution’s service and connecting to an external service provider)

- Providing users of the service, such as students, with clear guidance on what information is accessible to and used by the institution, and what information is accessible to and used by the service provider

- Ensuring users of the service sign up to use the service directly with the service provider and not through the institution. In this way, each individual can decide on the extent to which they wish to establish their own relationship with the service provider, and can withhold or disclose whatever personal information they wish

- Making participation in and contribution to the service optional for users – e.g. users can choose whether or not to contribute to a research wiki

Where users are to register individually, institutions should ensure prior to adopting a Web 2.0 service that the terms of service which users will be signing up to are appropriate for the UK legal environment. This is particularly important where use of the service is compulsory for a course. Institutions should not require users to sign up for Web 2.0 services which purport to require them to waive legal protections guaranteed by UK data protection law. Institutions should, when inviting users to register for a Web 2.0 service, provide clear guidance about the data protection implications of that registration; provide advice on the effective use of privacy enhancing elements of the service; and advice on how to unsubscribe and remove personal data from the service.

Depending on the nature and extent of use of a service, institutions may wish to give students a short briefing on the risks at the start of their course or provide appropriate information in the course handbook. Alternatively, it may be appropriate to include this sort of information in an institutional privacy policy.

Publication of Personal Information - Use of some Web.2.0 services may involve requiring users to publish their personal data on the Internet. Compulsory use of such services by institutions, or use of such services in circumstances which place users who do not wish to make such disclosures at a significant disadvantage, may breach the DPA 1998. This can be avoided by using services which let users conceal their identity, e.g. by allowing the use of aliases. However, withholding of names does not equate to anonymising data, and institutions should be alert to the risks inherent in requiring the disclosure of so much information that a user can be identified even in the absence of use of their name. Users should be clearly advised on what information will be published and what information will be available on a more restricted basis.

Transferring Personal Information Outside the EEA - Many Web 2.0 service providers are based outside the European Economic Area (EEA), e.g. in the United States. As a result, personal data supplied to those service providers is likely to be processed outside the EEA. While it is acceptable for individuals in the EEA to supply their personal data to non-EEA service providers, the DPA 1998 prohibits the transfer of personal data by data controllers to third parties outside the EEA, unless certain conditions are met.
In circumstances where institutions use Web 2.0 service providers, they should always ensure that they know where information that is supplied to the service providers will be processed, so that appropriate measures can be adopted. There are various methods of dealing with personal data transfers outside the EEA:

- In circumstances where a web service is to be used and users have a choice whether or not to sign up - the institution should ensure that its users are adequately informed about the data protection consequences of doing so.
- In circumstances where a web service is to be used and the user registers directly with the service, is aware of the overseas transfer, and has control over what information is provided to the service provider - the institution should ensure that its users are adequately informed about the data protection consequences of doing so.
- In circumstances where a web service is to be used, and the institution is providing user personal data to the service provider as a third party - the institution should consider whether:
  - the country in which the service provider is based has adequate protections for personal data in relation to the proposed transfer (see below).
  - the type of transfer is exempted from the general prohibition on transfers to non-EEA countries.
  - whether there is a need to negotiate a customised agreement with the service provider.
- In circumstances where a web service is to be used, and the institution is using the service provider as a data processor – the institution should negotiate a customised agreement with the service provider.

Appropriate mechanisms for doing this include privacy statements or course handbooks. Users must be able to opt out of the use of cookies and monitoring. If an externally-provided service is designed to appear to be part of the institution [e.g. a template has been used to apply institutional branding to a blog] the institution should ensure that people who register at that site (e.g. in order to post comments to the blog) understand that they are not just entering into a relationship with the institution, but also with the service provider. They should be given clear information as to what information is available to, and used by, which party.

Some service providers may make use of users’ details for advertising and marketing purposes. This can be annoying for users and, in cases where use of the service is compulsory or where the service provider is a data processor acting on behalf of the institution, may breach the Privacy and Electronic Communications (EC Directive) Regulations 2002. To minimise these risks, users should be given clear instructions on how they can opt out of advertising and marketing activities if they wish to do so. Institutions should avoid using services where it is not possible to opt out of advertising and marketing emails.

**Information Provision** - Under the DPA 1998 and related legislation, if an institution uses an external Web 2.0 service provider to collect information about or contributions from people on its behalf, it must provide clear information about:

- How the institution or other parties will use the information.
- Who will have access to or will retain copies of the information.
- What information will be generally accessible over the Internet.
- Any cookies that may be downloaded to the user’s computer.
- Any monitoring of an individual’s usage and activity in the service.
- The country that hosts the service (if the service is hosted outside the UK).

Information Retention - Personal data placed on Web 2.0 services based in non-EEA countries may, in some circumstances, be legally held indefinitely and the service providers may have no legal obligation to remove it. The DPA 1998 requires that the data controllers and data processors should keep information about people for no longer than necessary. Institutions should thus consider carefully if the Web 2.0 services they wish to use will expose the institution to liability for breach of the DPA 1998, or expose their users to unwanted long-
term personal data disclosure. Institutions should thus ensure that the Web 2.0 services that they wish to use have adequate data privacy guarantees concerning the appropriate removal and disposal of users' personal data after the purpose for which it was collected and processed has ended.

Additionally, where institutions have entered into arrangements with Web 2.0 service providers to provide particular services involving the processing of user personal data they should consider whether it is likely to be necessary to take down or delete information that has been posted to the service to prevent the processing of information likely to cause someone substantial damage or distress. Before signing up to a service, institutions should consider whether the terms of use and facilities of the external service will enable them to do this quickly, if necessary.

12.7 E-learning Systems - Virtual Learning Environments, ePortfolios

All e-learning systems will collect and process personal information about students at some point in the process. From the point at which a student starts using a virtual learning environment ("VLE"), most things they do in that VLE will generate personal data. In most cases, in respect of a VLE, the data controller for the personal data will be the educational establishment. Where the technical provision and administration of the VLE is outsourced to a third party provider, it is still likely that the institution will be the data controller, with the third party provider being considered a data processor acting on the institution's behalf.

Before an institution permits a student access to an e-learning system it must ensure that any data protection notice previously given to the student will allow the processing of that student's data in the system. If the existing data protection notice is insufficient then a separate data protection notice must be provided before the student starts using the e-learning system.

Because of the nature of the personal data processed by an e-learning system - not just student details, but potentially also the student's submitted work and their academic results, amongst other things - it is obviously vital that these data are securely maintained. From a technical standpoint e-learning systems must be robust and secure, as must the hardware, software, databases and communications systems on which they are based. Organisational measures must also be addressed, including who has access to the system, what controls are in place over how these people can access the system, and how the entire system is governed.

In addition to ensuring the security of its own processing, an educational establishment must also take steps to ensure that any data processors that process the data on its behalf are placed under security obligation. The Act requires that a contract must be executed in writing between a data controller and its data processors.

The data protection issues that are likely to arise from an institutional e-learning system will vary depending on a range of variables, for example, the developmental process that produced the system, the nature of the data it is envisaged will be stored in that system, the range of people who it is envisaged will have access to the data, and in the case of ePortfolios in particular, the means by which learners, rather than the institution may make the data available to others.

It is clear that for some types of e-learning system, such as ePortfolios, an institution may only host the e-learning system and not make decisions about the processing of personal data contained in it. In these circumstances the institution is probably not acting as a data controller and thus data protection legislation will not apply to its service provision. Where an institution does exercise some control over the data in the e-learning system, e.g. transcript data contained in an ePortfolio, it may be considered a data controller, and it will have to ensure that it complies with the DPA 1998.

End-users may also be considered data controllers in certain circumstances, for example where their ePortfolio contains personal data concerning third parties.

Ensuring best practice compliance with data protection law, should always be built into the planning/design process, when developing an e-learning system. Proposed uses of personal data, as well as potential 3rd
parties from whom transfers of personal data may be received into the system, or to whom data may be transferred from the system, should be identified and their respective data protection risks identified and the institutional responses documented. Institutional data protection officers should always be involved in this process.

When the e-learning system is operational the institution must take such steps as are necessary to ensure that it is able to demonstrate continued compliance with its obligations under the Data Protection Act 1998. Data subjects, institutional employees and 3rd parties permitted to access the personal data should all be regularly reminded of their rights and obligations as regards the system. All proposed future changes to the system, both technical and administrative, should be reviewed for their data protection implications prior to their implementation, and where necessary, advice on their impact should be sought from institutional data protection officers.

Further discussion and advice on ePortfolios, VLEs and data protection, including how to build data protection into the development process when implementing new elearning systems, can be found at: http://www.jisc.ac.uk/uploaded documents/Data Protection FAQ.pdf and http://www.jisclegal.ac.uk/pdfs/dataplawelearn.pdf.
13. Collection and Processing of Personal Data Relating to Disability

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

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

FE and HE institutions should provide:

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

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

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

14.1 Next of Kin/Emergency Contact Information

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

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

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

14.2 Counselling Services

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

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

- Guidance to the service’s personal data policies on data collection and retention
- Guidance on access to counsellors’ notes and other records that refer to them
- A timescale for destruction of the client’s personal data

FE and HE Employee and Student Counselling Services should:

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

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

- Where the counsellor has the express consent of the client to disclose the data
- Where the counsellor believes that the client is a serious danger to themselves, that their GP should be informed of that fact so that appropriate steps can be taken to ensure their safety, and that to inform the client of the disclosure would increase the level of risk
- Where the counsellor believes that serious harm may befall a third party if the data were not disclosed
- Where the counsellor would be liable to civil or criminal court procedure if the data were not disclosed
FE and HE Employee and Student Counselling Services may keep “risk registers” of various types, including:

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

Access by counsellors to such “risk registers” should be available only on a “need to know” basis. Inclusion on a “risk register” may not be disclosable to a data subject under subject access, on the grounds that the health & safety of the data subject, or counsellors, may be at stake (s. 31(2)(e)).

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

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

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

14.3 Careers Services

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

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

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

FE and HE institutions’ Careers Services should:

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

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

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

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

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

14.5 Alumni Records

While UK HE institutions do not yet pursue their alumni as assiduously as North American institutions, alumni are clearly a potentially valuable source of funding. An important first step is to be able to locate and correspond with them. Alumni offices often adopt practices resembling, or indeed identical to those of the direct mail industry. Where this is the case, an alumni office will have to ensure that its practices:

- Conform with the data protection principles
- Take account of the fact that data subjects can request that their personal data are not processed for direct marketing purposes
- Are in conformity with the requirements of the PECR 2003, where alumni are to be contacted by means of electronic communications

FE and HE institutions should ensure that:

- Students are informed at the time of the collection of their personal data for an alumni database of the purpose of that collection i.e. that the institution will wish to maintain contact with them after they finish their course of study
- Ideally, students and alumni are able to opt out of the collection and processing of their personal data for such purposes
- Students and alumni are able to request that where their personal data are collected and processed for alumni contact purposes, the data are not also processed for direct marketing purposes. For these purposes, the postal mailing of University magazines may not constitute "direct marketing." However, if the mailing is about a University credit card (an increasingly popular idea) that will be considered the direct marketing of products and services for which an opt-out would be required
- Where student and alumni data are used in electronic communications for direct marketing purposes (e.g. fundraising or campaigning), that the PECR 2003 rules are followed
- Students and alumni are provided with mechanisms whereby they can obtain the rectification, blocking, erasure, and destruction of their personal data, if necessary

FE and HE institutions may consider implementing mechanisms permitting students and alumni to access and correct their data remotely (e.g. passworded Internet access to their alumni database record) where adequate security measures are available.

14.6 CCTV and Similar Surveillance Equipment

FE and HE institutions are increasingly using Closed Circuit Television and similar surveillance systems (hereafter referred to as CCTV) across their sites to ensure site security and the safety of staff, students and visitors. Users of CCTV will need to comply with the provisions of the DPA 1998 as these systems invariably require the processing of personal data. The Information
Commissioner has issued a Code of Practice in accordance with his powers under s. 51(3)(b) of the DPA 1998 for users of CCTV and similar surveillance equipment monitoring spaces to which the public have access.


Compliance with this Code of Practice, notably those standards that are directly based on the Data Protection Principles and Act, will aid users of CCTV systems in meeting their legal obligations. Compliance with the Code of Practice will also factor into any determination by the Data Protection Commissioner as to whether institutions have made proper use of CCTV. The perception that only CCTV systems that involve significant automated processing, such as automated recognition, or automated scanning, are “processing” for the purposes of the DPA 1998 under the Act, is almost certainly incorrect given the wide definition of processing under s.1 of the DPA 1998. This definition is clearly much wider than ‘automated processing’.

FE and HE 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

14.7 Student Unions

The position of FE and HE institutions regarding compliance of Student Unions or similar bodies in relation to the DPA 1998 will be determined by whether or not those entities are considered to be an ‘integrated part’ of the institution, as determined by governing documents.

Any institution whose Students’ Union is an unincorporated association of that institution will be responsible for any processing undertaken by its Students’ Union. Students’ Union data processing activities will be included in the institution’s Data Protection notification, and the institution will need to apply appropriate controls (backed up with appropriate sanctions) to ensure that the Union complies with institutional data protection policy.

Where an institution’s Students’ Union exists as a wholly separate legal entity, that institution is not legally responsible for ensuring notification and supervising the DP activities of the Union. e.g. “old” universities whose constitutions make their Unions separate entities. In such circumstances the institution should be immune from prosecution should its Union contravene the law. However, it is advisable for institutions in such a position to offer advice and guidance to their Students’ Unions regarding data protection law, as the relatively rapid turnover of student officers and sabbaticals militates against the long-term retention of organisational DP knowledge.
15. International Transfers of Personal Data

15.1 Transfers of Personal Data to EEA Countries

Under the DPD 1995, States which are members of the EEA (the 27 EU Member States, plus Norway, Iceland and Liechtenstein) are considered to ensure an "adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." This means that transfers of personal data between those countries are automatically permitted.

In principle, the laws of the EEA States have been harmonised by their implementation of the DPD 1995 into their national laws. In practice, there remain significant legal and administrative divergences. Examples of differing legal definitions between the EEA States include those for such key terms as "data controller," "data processor," "sensitive data," "anonymous data," "consent," "third party," "establishment," and "equipment". It is unwise therefore to assume that transfers of personal data to, or from, other EEA States will always be unproblematic. Liaison with Data Protection Officers at institutions/organisations to which personal data is to be sent, or from which it is to be received, is thus advisable, as is seeking advice from the ICO, particularly where transfers involve sensitive personal data.

FE and HE institutions should, prior to beginning any personal data transfers to EEA States whether to other data controllers or to data processors:

- Evaluate the relevant national legal and administrative compliance criteria for personal data transfers in all States involved
- Liaise with appropriate officers in institutions/organisations to, or from, whom data is to be transferred, to allocate responsibility for ensuring that appropriate legal and administrative formalities have been satisfied
- Document both the legal and administrative requirements, and the agreed responsibilities of the respective parties, ideally in a contractual document, with appropriate warranties and indemnities in case of breach

15.2 Transfers of Personal Data to Non-EEA Countries

The DPA 1998 contains specific provisions with regard to the transfer of personal data to countries outside the EEA. The eighth data protection principle states "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." This is qualified by a number of conditions set out in Schedule 4 DPA 1998, for example, personal data may be transferred to a country without an adequate level of protection where the data subject has given his consent to the transfer.

When considering transfers of personal data outside of the EEA an institution will need to consider the following elements:

- Is there a transfer of personal data to a third country? Is that transfer necessary?
- Does the EU formally consider the non-EEA country to have an adequate level of protection?
- Do any of the other derogations to the Eighth Principle specified in Schedule 4 DPA 1998 apply (e.g. the consent of the data subject to the transfer)?
- Does the institution have, or can it put into place, adequate safeguards between itself and the other parties to protect that data (e.g. model clauses or binding corporate rules)?
- Do conditions in the third country, and the nature of the transfer, ensure that an adequate level of protection will be given to that data (e.g. national legislation in the jurisdiction to which the data are transferred; or codes of conduct at an industry or sectoral level; or elements of both)?

15.2.1 Formal Adequacy Rulings

Some countries outside the EEA have been officially deemed by the EU Commission to have an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data,
but the list is both eclectic and short. Countries with an official ruling of adequacy are Argentina, Canada, Switzerland, Guernsey and the Isle of Man. There is a partial finding of adequacy for the United States with regard to those organisations who have volunteered to be subject to the US/EU Safe Harbor principles. Details of the Safe Harbor Agreement and organisations that are covered by it can be found at - http://www.export.gov/safeharbor/.

No new findings of adequacy have been made since 2004, and the EU Commission has stated that it is unlikely that there will be any significant increase in adequacy rulings in the future. Formal adequacy findings therefore only provide a limited solution.

15.2.2 Schedule 4 DPA 1998 Derogations

The DPA 1998 provides for a number of derogations from the Eighth Principle, i.e. circumstances where the prohibition on the transfer of the personal data in question is not prohibited:

- The data subject has given his consent to the transfer
- The transfer is necessary for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller
- The transfer is necessary:
  - for the conclusion of a contract between the data controller and a person other than the data subject which is entered into at the request of the data subject, or is in the interests of the data subject, or
  - for the performance of such a contract
- The transfer is necessary for reasons of substantial public interest
- The transfer is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); for the purpose of obtaining legal advice; or is otherwise necessary for the purposes of establishing, exercising or defending legal rights
- The transfer is necessary in order to protect the vital interests of the data subject
- The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer
- The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects
- The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects

It is likely that only a limited sub-set (the first 3) of these derogations will be available to FE/HE institutions in the normal course of their business. The final two derogations are dealt with in the section below.

15.2.3 Use of Model Clauses or Binding Corporate Rules

Where an exporting institution has no formal ruling of adequacy on which to rely, the use of Commission-authorised standard contracts (‘model clauses’) may enable the transfer to be exempted from the restrictions of the Eighth Principle, on the basis that the model clauses provide adequate safeguards for the rights and freedoms of data subjects.

The Commission has approved 3 sets of model clauses:

The model clauses contain obligations on both the data exporter and data importer to ensure that the transfer complies with the standards required by the Directive and the data subject has a right to directly enforce its rights under them.

Under s. 54(6) DPA 1998, the ICO has issued authorisations stating that the Eighth Principle does not apply where the transfer has been made using any of the model clauses. This means that an exporting data controller who uses these model clauses does not need to make a separate assessment of adequacy in relation to the transfer.

Parties are free to include any other clauses on business related issues provided that they do not contradict the model clauses. However, changing the wording of the model clauses in any regard, even if it does not alter the intended meaning or effect of any clause, means they will not be automatically authorised, unless the change is to make the contract between more than two parties (e.g. where there is more than one data importer) and provided that the obligations of all the parties remain clear and legally binding.

Use of non-standard contracts will require the data controller to make a separate positive assessment of adequacy in relation to the transfer, or to obtain authorisation from the ICO.

Binding corporate rules (BCR) are internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards for the rights and freedoms of data subjects. BCR must be submitted for approval by the Commissioner in order to obtain an authorisation which provides that transfers from the UK may be made within the group on the basis of the BCR. They are unlikely to be suitable for most forms of FE/HE overseas personal data transfers.

15.2.4 Data Controller Assessment of Adequacy

In the absence of any other option, it is always open to an organisation to determine for itself that the transfer it wishes to make will provide adequate safeguards. There will be three primary elements involved when determining the adequacy of protection of data privacy in a non-EEA country to which personal data are to be transferred:

- The nature of the data and the purpose[s] for which it is to be processed
- The substantive rules that apply to protection of the data
- The methods of enforcement by which compliance with those substantive rules is attained

The adequacy assessment must be made both in terms of the country to which the data is to be transferred and the organisation[s] to which it is to be transferred. Such an assessment might include:

- The extent to which national legislation in the jurisdiction to which the data are transferred provides for protection for all, or specific types of personal data (e.g. educational information, or medical data)
- If the sector within which the organisation to which the data is to be transferred has specific professional rules or codes of conduct at an industry or sectoral level
- The fact that there are specific contractual data protection provisions between the UK-based transferor and the transferee, even if these are not EU-approved model clauses

Independent data controller assessments are more risky that the other 3 approaches, because any decision on adequacy will necessarily be subjective, and may be overruled by the ICO or the courts. The data controller has to take full responsibility for the assessment, and carrying out an effective assessment will inevitably be resource and time intensive.
When considering a transfer of personal data to a non-EEA country FE and HE institutions should:

- Determine whether the country in question has been formally assessed by the EU Commission as having adequate protections for the rights and freedoms of data subjects in relation to the processing of personal data
- Where the country has been formally assessed as providing adequate protections, treat the transfer as they would personal data transfers to EEA States, whether to other data controllers or to data processors
- Where the country has not been formally assessed as providing adequate protections, consider whether the proposed transfer is exempted from the Eighth Principle by virtue of the Schedule 4 derogations. Examples in the FE and HE sector might include: requests by FE and HE institutions to non-EEA governments, agencies, and organisations for information necessary to determine academic eligibility for attending a course of study in the UK; transfers of personal data to non-EEA governments, agencies, and organisations sponsoring students to attend a course of study in the UK, where such sponsorship is dependent upon attendance and/or performance criteria; transfers of personal information (e.g. examination marks), relating to, and required by, data subjects engaged in distance learning courses
- Fully document any decision they make about the use of the Schedule 4 exemptions, in case it is necessary to justify the basis for any transfer to a third country to the ICO or courts

FE and HE institutions should consider the potential benefits of obtaining the specific and informed consent of the data subject before transferring personal data to a non-EEA country, that is:

- The data subject can be made aware of the risks that the institution may have assessed as being involved in the transfer; and
- The data subject is able to give their clear and unambiguous consent to the transfer

The institution should be able to produce clear evidence of the data subject’s consent in any particular case and be able to prove that the data subject was informed as required.

Consent in writing is thus recommended, unless the institution has suitable technological means to ensure that authenticated consent can be collected on-line. An example in the FE and HE sector would be the transfer of staff personal data to a non-EEA country to be used in the management of a distance learning course. Where a data subject requests a reference be written and sent to a non-EEA country, the request itself will indicate their consent to the personal data transfer.

FE and HE institutions should:

- Evaluate whether the use of Commission-authorised model clauses will be an effective means of permitting the transfer of personal data to non-EEA countries, particularly in circumstances where obtaining specific consent from data subjects is impractical or unreasonable

Where FE and HE institutions operate overseas campuses in non-EEA countries that are formally part of the institutions, they should consider whether a Binding Corporate Agreement could be used to permit the transfer of personal data.
FE and HE institutions should:

- Have particular regard to the recommendations in the ICO’s guidance documentation when determining whether or not a country has adequate protections for personal data in relation to the proposed transfer
- Establish clear and documented institutional procedures and administrative responsibilities for the transfer of personal data to non-EEA countries
- Consider whether or not and, if so, the extent to which, a decision to treat the third country as adequate in relation to the proposed transfer will prejudice the fundamental rights and freedoms of the data subject(s), and in particular their right to privacy with respect to the processing of personal data
- Fully document any decision they make about the self-assessed adequacy of a non-EEA country’s protections for personal data, in case it is necessary to justify the basis for any transfer to a third country to the ICO or courts

FE and HE institutions should not:

- In the absence of a sponsorship arrangement or other agreement between the data subject and a third party, disclose personal data requested by non-EEA governments, agencies, and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas, without the specific and informed consent of the data subjects concerned
- Disclose personal data requested by non-EEA governments for the purposes of determining liability to attend National Service, without the specific and informed consent of the data subjects concerned

16.1 In Scotland & Northern Ireland

The foregoing guidance for FE and HE institutions is of general application. Although there are certain specific provisions for Northern Ireland and Scotland contained in the DPA 1998, these largely relate to issues outside the scope of the guidance. Mention is made of relevant issues as appropriate.

16.2 To Individuals Under the Age of 18

Rights under the DPA 1998 are not subject to a minimum age requirement for applicants. Children can make a subject access request if they are capable of understanding the nature of the request. A parent or guardian can only apply on the child’s behalf if:

- The child has given consent
- The child is too young to have the understanding to make an application

s.66(2) of the DPA 1998 states that in Scotland there is an automatic presumption that a person of 12 years or more is of sufficient age and maturity to understand and exercise their rights under the Act.

16.3 To Foreign Nationals

Rights under the DPA 1998 are not subject to UK citizenship. Any Data Subject whose personal data is being processed by, or on behalf of, a UK-based Data Controller can rely on the provisions of the Act, even where the processing is carried out by a Data Processor which is based outside the UK.

17. Retention of Records Containing Personal Data

The area of records management in FE and HE has seen considerable development since 2000. This has been driven in large measure by the DPA 1998, the FOIA Acts, and the Environmental Information Regulations 2004, as well as a growing recognition of the complexity of the data retention requirements of the legislative and regulatory framework within which institutions operate. Previous iterations of this Code of Practice contained a simplified version of the JISC Records Retention Schedule (RRS). Readers are now advised to refer directly to the JISC Infonet webpages relating to the Business Classification Scheme (BCS) and Records Retention Schedules (RRS) for Further and Higher Education Institutions at –

http://www.jiscinfonet.ac.uk/projects/records-retention-fe/index.html and http://www.jiscinfonet.ac.uk/partnerships/records-retention-he

and, in particular, the Records Retention Schedules at –


Readers in Scotland should also refer to the Guidance Note on the Impact of the Prescription and Limitation (Scotland) Act 1973 on the retention of records at:

http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-pla-guidance

and the revised version of the HE Records Retention Schedule, including suggested amendments to the recommended retention period based on the Guidance Note at:

http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-rrs-pla
### Glossary and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 29 Working Party</td>
<td>An advisory group, set up by the DPD, composed of representatives of the data protection authorities of the Member States. It acts independently and examines any questions concerning the application of the national measures adopted under the DPD to foster the uniform application of such measures.</td>
</tr>
<tr>
<td>BAC</td>
<td>British Association for Counselling</td>
</tr>
<tr>
<td>BPS</td>
<td>British Psychological Society</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>DCSF</td>
<td>Department for Children, Schools and Families</td>
</tr>
<tr>
<td>Direct marketing</td>
<td>The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. (DPA 1998 s.11)</td>
</tr>
<tr>
<td>ePortfolio</td>
<td>A collection of electronic evidence assembled and managed by a user as a learning record that provides actual evidence of achievement.</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area – the 27 EU Member States, plus Iceland, Liechtenstein and Norway.</td>
</tr>
<tr>
<td>EU</td>
<td>European Union – Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>FPS</td>
<td>Fax Preference Service</td>
</tr>
<tr>
<td>FE</td>
<td>Further Education</td>
</tr>
<tr>
<td>HE</td>
<td>Higher Education</td>
</tr>
<tr>
<td>HESA</td>
<td>Higher Education Statistics Agency</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>JANET(UK)</td>
<td>The trading name for the JNT Association, which has responsibility for the management of the UK’s Higher Education networking programme. It manages the operation and development of the JANET network, under a Service Level Agreement from JISC.</td>
</tr>
<tr>
<td>LBPR 2000</td>
<td>Telecommunications [Lawful Business Practice] [Interception of Communications] Regulations 2000</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service [text messaging]</td>
</tr>
<tr>
<td>TPS</td>
<td>Telephone Preference Service</td>
</tr>
<tr>
<td>VLE</td>
<td>Virtual Learning Environment</td>
</tr>
</tbody>
</table>