the national archives

Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998

Susan Healy
The National Archives
Kew Richmond Surrey TW9 4DU

Email susan.healy@nationalarchives.gov.uk

TABLE OF CONTENTS

1 INTRODUCTION

1.1 The Data Protection Act 1998, passed on 16 July 1998, was brought into force on 1 March 2000, with transitional exemptions extending to 23 October 2001 and 23 October 2007 and some indefinite exemptions. This Act replaced the Data Protection Act 1984, which it repealed, in its entirety. Together with a growing volume of secondary legislation and case law the Data Protection Act 1998 (henceforth abbreviated as the Act) and amendments made to it by other legislation constitute United Kingdom data protection law. Particular note should be made of amendments through the Freedom of Information Acts which primarily affect bodies subject to those Acts (public authorities).[1]

1.2 Anyone who determines the purpose for, and the manner in which information about identifiable living individuals is processed has to comply with data protection law in managing that information, unless exemptions apply, as with unstructured manual data or data held for domestic purposes only. Information about virtually everyone now living in the United Kingdom - as in many other countries - is recorded on numerous computer databases, in many paper files and also within emails and word processed documents on personal computers. Data protection law permits individuals to know what personal information is held about themselves and to correct it if necessary, and ensures that other people do not have unauthorised access to that information. In this way the law attempts to preserve the information privacy of individuals whilst allowing organisations that collect and process personal data to pursue their legitimate interests.

1.3 The main burden falls on organisations with large client bases or large numbers of staff, such as government departments, local authorities, financial institutions and public utilities, but any company, organisation or single person who determines the purpose for and manner in which personal information is processed, however innocuous, will need to adhere to the Data Protection Act 1998.

1.4 Records managers are clearly most immediately concerned but archivists may well have records passed to them which contain

[1] There are two such Acts, the Freedom of Information Act 2000, which applies to all UK public bodies except for those that fall under the Scottish Parliament or any part of the Scottish Administration or are otherwise considered Scottish bodies, and the Freedom of Information (Scotland) Act 2002. Some of the amendments to the Data Protection Act automatically apply to data held by Scottish public bodies through the UK FOI Act; others are made to apply by SI 2004 No. 3089, The Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004. Any references in this Code of Practice to the Freedom of Information Act or FOI Act refer to both Acts unless otherwise specified.

information about individuals who are still alive (e.g. school admission registers, court records, hospital records) and may themselves create relevant databases, electronic documents or paper files of personal information that are subject to the Act (e.g. search room attendance registers, correspondence with private owners of archives). Both records managers and archivists need to understand the general principles that govern personal data and its management and to ensure that their handling of it complies with the Act.

1.5 The Act provides for the Information Commissioner to facilitate compliance with it by co-operating with "trade associations" in preparing "codes of practice for guidance as to good practice" (section 51(4)). Following consideration of this code, the Information Commissioner has expressed the opinion that, by providing clear authoritative advice, it promotes the following of good practice.[2] It is a statement of good practice issued following some experience of the working of the Act. As such it will carry considerable weight in the event that the actions of records managers and archivists are challenged. Departure from its provisions is not unlawful but will need to be justified in terms of compliance with the Data Protection Act 1998.

1.6 The Code is not intended as a general guide to the Act nor a guide to the duties of Data Protection Officers or Co-ordinators. Its focus is as follows:

- To explain how data protection must be integrated into corporate information and security policies (chapter 2)
- To provide guidance for the processes that records managers carry out in the order in which they need to be addressed from the point of view of records managers (chapter 3)
- To provide similar guidance to archivists, where this is different from the guidance applicable to records managers (chapter 4)
- To explain terms used in the Act and this Code (Annex A)
- To draw attention to the main provisions of the Act insofar as they affect records managers and archivists (Annex B)
- To provide specimen forms and forms of word (Annex C)

[2] The Code was originally drafted by a joint working party composed of representatives of the Society of Archivists, the Records Management Society and the Public Record Office (later The National Archives). The following served on the working party: Jerome Farrell (to July 1999), Susan Healy (convenor from 2001), Vanora Hereward, Stephen Howard (from December 1999), Joanne Ichimura (from February 2000), David Johnson (convenor until 2001), Serena Kelly (to August 2000), James Lappin (from July 2000), Mike Marsh (from July 2000), Julia Sheppard (to June 2000), Paul Sillitoe (to June 2000), Helen Wakely (from June 2000), Gillian Whichelo (to June 2000). The working party came to an end in 2002 and subsequent editing was undertaken by Susan Healy.

1.7 The Code covers the entire records life cycle and addresses records in all media, but issues unlikely to affect records managers and archivists have not been dealt with. Some data, for example of the police, credit reference agencies, etc, is subject to particular restrictions; these have been indicated but those working in specialist repositories will probably need to seek additional specialist advice.

1.8 The Code of Practice is intended to be used in conjunction with the Act, secondary legislation (such as Regulations) and guidance published by the Information Commissioner. It is the responsibility of records managers and archivists to familiarise themselves with these sources (see Annex D for details) and to seek legal advice when necessary. This code of practice does not itself constitute legal advice.

2 CORPORATE RESPONSIBILITY

The purpose of this chapter is to summarise the responsibilities of the organisation in relation to personal data. The professional responsibilities of records managers and archivists are dealt with in chapters 3 and 4.

2.1 Responsibilities for data protection

The primary responsibility for ensuring that the collection and processing of any set of *personal data* comply with the Act, and in particular with the Data Protection Principles (for which see Annex B, B1), rests with the *data controller* (see Annex A), which can be an individual or another type of legal person such as. a company or a local authority. *Data processors* act only on behalf of the data controller under contract and their obligation is to observe the terms of the contract. Most organisations appoint their own data protection officer to oversee compliance within the organisation and this person will ensure that the organisation issues to all employees a corporate data protection policy and procedures for handling personal data. He will also ensure that employees receive appropriate training on data protection issues. All employees are responsible for ensuring that their own collection and processing of personal data and *sensitive personal data* are in accordance with these procedures. (See Annex A for explanations of italicised terms.)

2.2 Collection and processing of personal data (Principles 1, 2 and 3)

2.2.1 Data subjects have the right to be informed of the identity of the data controller and the intended purposes of processing (Principle 1). Anyone deliberately collecting personal data should be candid about why they are doing so and how they intend to use the data. Any form used to collect personal data, whether paper or electronic, should provide the person contributing the data with:

- The identity and address of the data controller
- A brief description of the purposes for which the data will be used
- Any further information that is relevant in the particular context. This can include:
    - If it intended to disclose data to third parties, details of them and their declared purposes, with an opportunity to indicate consent or dissent

- If it is intended to transfer the data out of the European Economic Area (EEA) on the basis of consent, an opportunity to give such consent
- Details of how to seek access to the data and to correct any inaccuracies in it

2.2.2 This information must be clearly written in plain English (and, if necessary, in other languages) and prominently placed on the data collection form. A sample copy of any form used to obtain data should be kept for as long as the data itself.

2.2.3 If the data is not collected in written form, for example if it is collected during a telephone call or some other oral contact or by use of a recording device such as CCTV, the person collecting the data must still ensure that the obligations outlined at 2.2.1 are met. The Information Commissioner has produced specific guidance on personal data recorded by means of CCTV cameras (see guidance listed at http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx).

2.2.4 Data should be collected only if it is needed for the intended purpose (Principle 3). Excessive or irrelevant data should not be collected simply because it may be useful at some point in the future. For example, visitors should be asked to enter in a search room attendance register only the details required for it to serve as an accurate record of their presence in the search room. Another aspect to consider is whether anonymous information would achieve the same result as information with a name attached. For example, for the search room register to fulfil its purpose the names of visitors are needed but a survey questionnaire may not need the name of the person completing it. Records of decisions of this nature should be kept for as long as the data itself.

2.2.5 Collection and processing of personal data should be capable of being justified by one of the conditions set out in Schedule 2. The conditions most likely to be used by records managers and archivists are:

- The data subject has given consent to process the data
- The processing is necessary to ensure compliance with a legal obligation other than an obligation imposed by contract
- The processing is necessary for the performance of a contract to which the data subject is a party
- The processing is necessary for the exercise of any functions conferred by any Act, or the functions of the Crown, a Minister of the Crown or a government department or for the administration of justice

- The processing is necessary for the legitimate interests of the data controller or third party recipients and is not prejudicial to the rights and legitimate interests of the data subject

Note that these conditions need not be met when the processing is of category (e) personal data, i.e. manual data that is not part of a relevant filing system (see Annex A for an explanation of the different categories of personal data).

2.2.6 Processing of sensitive personal data should be capable of being justified by one of the conditions set out in Schedule 3 (or in a Statutory Instrument made under Schedule 3) as well as by a condition in Schedule 2. The conditions most likely to be used by records managers and archivists are:

- The data subject has given explicit consent to the processing
- The processing is necessary to protect the vital interests of the data subject or another person and consent cannot be obtained
- The processing is necessary to comply with employment law
- The processing of personal data relating to racial or ethnic origin is necessary to monitor and promote equality of opportunity
- The data has been made public as a result of steps deliberately taken by the data subject
- The processing is necessary for the exercise of functions conferred by any Act, or the functions of the Crown, a Minister of the Crown or a government department or for the administration of justice
- The processing is undertaken for medical purposes by a health professional or someone owing an equivalent duty of confidentiality
- The processing is allowed by the terms of SI 2000 No. 417, The Data Protection (Processing of Sensitive Personal Data) Order 2000, paragraph 9. This allows processing for research purposes in accordance with specified conditions; see 4.2.5 for details).

Again, these conditions need not be met when processing category (e) personal data.

2.2.7 As long as processing is otherwise fair and lawful, compliance with 2.2.5-2.2.6 above constitutes the authorisation for records managers and archivists to do their jobs.

2.2.8 If consent is the condition being relied upon, note that it must result from active communication and cannot be inferred from a failure to respond. If a data subject fails to indicate that he does

not consent, this must not be taken as an indication that he does consent to the processing of data. It is therefore important to ensure that relevant forms are signed. Where data is obtained electronically, it should be necessary to acknowledge a privacy statement and consent areas before data can be sent. Withholding consent to a subsequent incompatible use of the data should not be made onerous, e.g by requiring the data subject to write a letter to be removed from a mailing list. Evidence of the form of consent, or documentation of alternative justifications, should be kept for as long as the data. .

2.2.9 If data is collected from third parties, a check should be made of whether the data subject has authorised provision of the information. If so, obligations to inform the data subject of the processing may be waived.

2.3 Notification

2.3.1 The provisions relating to notification are found in Part III of the Act and in SI 2000, No. 188, The Data Protection (Notification and Notification Fees) Regulations 2000, as amended by SI 2001 No. 3214. For information about notification, templates for on-line notification, and the Register of Data Controllers, see http://www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx .

2.3.2 It is the responsibility of the data controller to notify all processing operations that involve personal data to the Information Commissioner. Notification is renewed annually and amendments should be made as necessary. Data processors are not required to notify.

2.3.3 There is no requirement to notify processing operations where the only personal data held by the organisation fall into one of these categories:

- Manual data (categories (c), (d) and (e) as defined at Annex A)
- Personal data in a public register or covered by one of the notification exemptions in SI 2000, No. 188, Schedule, paragraphs 2-5

However, organisations may wish to consider voluntary notification and, in any case, data controllers who are exempt from notification are still obliged to comply with the rest of the Data Protection Act and have a duty to make available on request all information that would have been included in the notification.

2.3.4 The exemptions outlined above will be particularly relevant to archivists as many archive holdings consist mainly (although not exclusively) of manual data. Archive holdings containing electronic records are likely to require notification (see 2.3.7).

2.3.5 The fact that a data controller has properly notified a type of data and the purpose or purposes of processing does not mean that any processing of that data for those purposes will be fair and lawful. All processing must, irrespective of the notification, be fair and lawful.

2.3.6 Where notification is required (or the organisation chooses to notify voluntarily) the data controller must provide a general description of the processing of personal data under the headings set out in the Information Commissioner's *Notification Handbook*. They include:

- The purposes of processing
- A description of the data subjects
- A description of the data classes
- A list of recipients
- Information about whether the data is to be transferred outside the EEA
- A statement concerning security arrangements

The description will be structured by reference to the purposes of processing. The *Notification Handbook* provides a list of "purpose titles" with which to categorise processing operations. For finding aids the purpose "Information and databank administration" should be used.

2.3.7 For those categories of processing that do not fit the standard purpose descriptions, a "special purpose" description can be approved by the Information Commissioner. He has approved the following special purpose description for archives :

"Records selected for permanent preservation as archives, with a view to their use in historical or other research"

Under this single special purpose description all archives held by an organisation can be notified, including those containing sensitive personal data. The description has been approved to cover:

- Public records in the custody of The National Archives
- Public records selected for preservation and transferred to other archive offices which have been appointed as places

of deposit for public records under section 4 of the Public Records Act 1958

- Other public sector archives such as the records of local authorities and of other bodies of the kind set out in Schedule 1 to the Freedom of Information Act 2000, and their Scottish equivalents
- Archives of private sector bodies, for example those of businesses or private research institutes, or of individuals. These archives might be in public sector archives offices or in private sector archives offices such as the Wellcome Library for the History and Understanding of Medicine.[3]

2.4 Maintaining accuracy of personal data (Principle 4)

2.4.1 Personal data held for operational purposes should be accurate and kept up-to-date. The difficulties of ensuring total accuracy are recognised and a realistic approach is adopted in the Act by requiring "reasonable" steps to have been taken to ensure accuracy. A culture of carefulness should be fostered within the organisation.

2.4.2 When collecting data, a decision should be made about quality control procedures to be used to check its accuracy. If the data comes from third parties, its likely reliability and accuracy should be assessed. Personal data supplied by the data subject need not be checked for data protection purposes. The procedures and the results of the checking should be documented and the documentation should be retained for as long as the data is retained.

2.4.3 Procedures must be in place to allow data subjects to correct inaccurate data and data subjects must be provided with information on how to exercise their rights to seek correction. If a data subject states that data relating to them is inaccurate and can provide evidence to support this contention, and the data is still in operational use, the correction should be made. Depending on the nature of the data, it may be necessary to record the fact of the correction and retain the incorrect data. For example, a simple change of address may require no formal record of amendment but something more complex that could impinge on the rights of the data subject should be recorded and the incorrect information previously used for decision-making should be retained. For data that has been archived see 4.7.

2.4.4 Third parties to whom inaccurate data has been passed may need to be informed of any corrections to the data. This will

[3] See 2.2.6 (last bullet point) concerning the legal justification for the processing of sensitive personal data by private sector archivists

depend on the nature of the data and whether the recipients are still likely to be using it. For example, if data was disclosed to a third party in connection with a job application some years ago, sending a correction is unlikely to be necessary. The guiding principle is that the legitimate interests of the data subject must be protected.

2.5 Retention or destruction of personal data (Principle 5)

2.5.1 Personal data should not be kept for longer than it is needed. The need to keep data relates either to the original purpose for collecting it or to a subsequent purpose, such as continued business use, that can be justified in terms of the conditions at 2.2.5-2.2.6 above and is otherwise fair and lawful. See also 3.3 and, for data that has been archived, 4.2.

2.5.2 Emails in personal mailboxes should not be retained indefinitely. Any emails required for the corporate record should be filed in an electronic records management system or printed out and placed on a paper file, then deleted from the personal mailbox. Personal emails should be filed in personal filing systems if required for future reference. Organisations with a centralised email system can arrange for automatic destruction on a rolling basis, e.g. of emails that are older than three months. Emails stored in an email vault system should also be destroyed on a regular basis.

2.5.3 Personal data for which a subject access request has been received by a body subject to the FOI Acts must not be destroyed, altered or concealed in order to prevent its disclosure to the data subject. Note that this does not prevent routine destruction as part of an orderly records management programme.

2.6 Inventory of personal data systems

2.6.1 Control over retention and destruction presupposes knowledge of what personal data is held by the organisation. Initially this information should be gathered by means of a comprehensive audit. Audit forms should record the source of the data, its purpose or purposes and its storage, access, security, retention and disposal arrangements. It is recommended that the audit information be maintained within an electronic spreadsheet or database.

2.6.2 The Act applies to a wide range of record types so the inventory should cover electronic and manual records. Electronic records

may include email, microforms, CCTV footage, videotape, CD, DVD, fax or voice-mail.

2.6.3 Those creating discrete sets of personal data should be encouraged to report them to the Data Protection Officer so that the inventory can be kept up to date; a model report form is at Annex C.

2.6.4 In the event of uncertainty as to whether personal information is personal data under the Act, or whether personal data falls within category (c) or (e), a risk assessment should be made based on whether a decision not to treat the information as being covered by the Act or part of a particular category will prejudice the individual concerned. If any doubt remains it is best to exercise caution and ensure compliance.

2.7 Data subject access to personal data (Principle 6)

2.7.1 Under section 7 of the Act, data subjects have the right to know what data is held about them and how it is being processed and to see the data in intelligible form. Requests for access should ideally be dealt with through a central point that will usually be the organisation's Data Protection Officer. If responsibility is devolved, requests should be dealt with in accordance with central guidelines and under overall central supervision. All employees should be made fully aware of data subject rights and of the procedure for responding to data subject access requests.

2.7.2 The following checklist may be useful:

(a) Written guidelines and training should be provided to staff responsible for dealing with data subject access requests. The guidelines should include:

- Clear instructions on how to respond to a request
- Details of data exempt from subject access (for which see Annex B, B4)
- Details of the fee that can be charged - the maximum fee payable is currently £10, except for accessible records (health and education records) for which there is a maximum fee of £50 for permanent copies (but see also 2.7.3)
- The statutory deadline for response - at most, 40 calendar days from the date the request was received and the fee paid

(b) Clear guidelines should be available to data subjects on how to make a data subject access request:

- Requests must be made in writing and a form can be provided although its use cannot be required (see Annex C for a model form)
- The applicant should supply enough information for the personal data to be located and identified. For example, former members of staff should be able to give rough dates of employment, while others should be able to indicate why the organisation is believed to hold information about them, which will help narrow the request. Archives offices will, in particular, need to know whether the data subject believes he features in the organisation's administrative records or in the archives
- Fee arrangements should be explained
- The statutory deadline for response should be explained

(c) Verification procedures should be in place:

- The identity of the person making a subject access request should be verified. The level of verification will depend on the sensitivity of the data being requested and the nature of the request and should not be unduly onerous. For example,a driving licence, passport or national identity card have a higher level of verification than a photopass. If the request is for CCTV images a photograph would be enough to prove identity. A recent letter or bill from a utility company can be used for evidence of the current address. Originals are preferred but copies are acceptable
- The authorisation of a person claiming to be acting on behalf of a data subject should be verified, e.g. through a letter signed by the data subject, with some means of showing it is genuine

(d) The interests of other people should be respected

- It is important to establish whether any restrictions or exemptions from disclosure apply. Exemptions are set out in Part IV of the Act. Particular care must be given to disclosure of data that might reveal the identity of another person in circumstances in which this would be unfair. In this case, the consent of the other person should be obtained for disclosure to proceed or their information should be redacted

(blanked out) unless the data controller is confident that it is "reasonable" to proceed without doing so.

- Guidance on dealing with subject access requests involving other people's information is on the Information Commissioner's Office website from this page: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx .

(e) Format and special needs should be considered

- The information provided must be intelligible – an explanation of any codes or specialist terminology may be required
- The information must be in a permanent form unless providing it in a permanent form is not possible, would involve disproportionate effort or the data subject agrees otherwise (see section 8 of the Act). Note that if the information is not to be provided in permanent form it must be provided in some other form
- There may be a need to consider whether the applicant has any special needs that should be met, e.g. the supply of information in a language other than English or in a special format, or provision of access away from the public gaze to documents considered likely to cause distress. In some cases special requirements may be protected by law, e.g. the Welsh Language Act 1993 or the Disability Discrimination Act 1995.

2.7.3 Special provisions apply when the request is to a public authority and relates to unstructured personal data in manual records that are not part of a relevant filing system. Note that a distinction must be drawn here between wholly unstructured data and relatively structured data, i.e. data that is structured to a certain extent but not sufficiently to make it part of a relevant filing system. Both fall within category (e) personal data but the former benefits from special provisions with regard to subject access requests in that there is no obligation to respond if either of the following applies:

- The applicant has not described the information sought
- The cost of responding would exceed a cost limit set out in SI 2004 No. 3244, The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004. The limit is currently set at £600 for bodies that are listed in Part 1 of Schedule 1 to the UK Act and £450 for all other

public authorities, including those subject to the Scottish FOI Act.

Relatively structured personal data, on the other hand, is subject to the same subject access provisions as category (c) data. (See Annex A for an explanation of the different categories of personal data.)

2.7.4 Requests for access should be monitored and recorded for performance measurement, audit and statistical purposes.

2.7.5 The Act provides no right of access for third parties. The issue of when and how access should be provided to third parties is covered at 4.9 below.

2.8 Security of personal data (Principle 7)

2.8.1 Personal data should be stored securely so that confidentiality is maintained at all times. Access should be provided only to those who have a need to know that can be satisfied within the law. The level of security should be appropriate and proportionate to the nature of the data and the harm that could arise from a breach in security. Risk management techniques should be used to assess the nature, level and impact of risks and the appropriate measures to be taken to protect the data.

2.8.2 The corporate information security policy should reflect the organisation's obligations under the Act and adoption of BS ISO/EIC 27001:2005, *Information technology. Security techniques. Information security management systems. Requirements* should be considered. Organisations can demonstrate compliance with this Standard by using one of the certification scheme run by the British Standards Institution and other bodies (see http://www.iso27001certificates.com/ for details). These enable an independent third party to certify organisational security arrangements against the requirements set down in the Standard.

2.8.3 Many breaches are accidental and result from insider action or inaction. The emphasis therefore should be on awareness raising, education and training so that information security is embedded in organisational culture and hence in employees' approach to the personal data encountered in their daily work. This should be extended to temporary staff whose work brings them into contact with personal data. Security breaches should be recorded and investigated and staff should be encouraged to report and respond to security incidents.

2.8.4 Access to sensitive personal data should be provided only to those whose reliability has been ascertained through screening and verification checks. Written contracts imposing appropriate levels of security should be in place for any processing undertaken by data processors.

2.8.5 Practical security measures to be considered include installing physical security devices such as electronic passes and intruder alarms, restricting access to secure areas, enforcing a clear desk policy in office areas and keeping a record of visitors and supervising their activities as far as possible. Electronic data should be secured, e.g. by means of software protection against viruses and Trojans, password-controlled access for authorised users only, and locking of unattended computers. Personal data should be transmitted securely: sealed or double envelopes should be used for manual personal records and encryption tools should be used for secure transmission of electronic personal data. Access restrictions applying to manual records should be clearly indicated in a prominent position.

2.8.6 Unwanted documents should be disposed of securely as confidential waste, e.g. by shredding, pulping, or incineration. Electronic data should be disposed of securely and in such a way that it cannot be reconstructed through the use of recovery utilities. This includes deleting and over-writing and physically destroying floppy disks and tapes

2.9 Transfer of personal data outside the EEA (Principle 8)

2.9.1 Transfer of personal data outside the European Economic Area (EEA) can be considered lawful only if the country or territory of destination ensures an “adequate” level of protection for the rights of the data subject in relation to the processing of personal data. See Schedule 1, Part II, paragraph 13 for things the data controller should consider in assessing adequacy and Schedule 4 for cases where the 8th Principle does not apply; the last includes the case that the data subject has given consent to the transfer.

2.9.2 It is important to note that “transfers” include making personal data available internally and externally to the organisation. Manual and electronic data transfers alike will be caught, including communication by email. For the position with regard to placing personal information on a website see 2.10.4.

2.9.3 So far, the European Commission has approved Switzerland, Argentina, Guernsey, the Isle of Man and, for certain activities,

Canada as countries which provide adequate levels of protection. The Commission's decisions can be found at:

http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

2.9.4 Transfer of personal data to the United States is possible under the Safe Harbor arranged by the European Commission and the US Department of Commerce. This enables lawful transfer of data to US organisations that have signed up to comply with a set of data protection principles and to follow agreed guidance. Details of the scheme are available on the Information Commissioner's website and at the europa website above. They are also available on the US Department of Commerce website at http://www.export.gov/safeHarbor/index.html.

2.9.5 The Act provides for transfers to non-approved countries if they are made on contractual terms that are of a kind approved by the Information Commissioner. The European Union has approved separate standard contract clauses for data transfers to data controllers and data processors non-EU countries, see:

http://www.europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

If there is any proposal to depart from these standard clauses legal advice on the wording of contracts should be sought.

2.9.6 The data controller is responsible for establishing whether transfers outside the EEA will be within the law, and should include information on these transfers in the corporate notification. Full records of all such transfers should be maintained, and the data subject informed upon request.

2.9.7 See 4.13 for particular issues arising in connection with archives.

2.10 Websites

2.10.1 All websites should include a privacy statement which sets out the organisation's policy with regard to the use of personal information about virtual visitors that is captured automatically. This statement should include provisions for use of "cookies" and log files. However, a privacy statement on a separate webpage is not enough. Basic messages and choices, at least, should be displayed in an intelligible and prominent way wherever personal data is collected, even if a more detailed explanation is provided elsewhere in a privacy statement.

2.10.2 The statement should also explain the organisation's intentions concerning personal information gathered as a result of direct email facilities or through on-line completion of forms, and provide an opportunity to opt out of subsequent contact from the organisation on different matters (see 2.2). A record of the conditions under which personal information was obtained should be retained for as long as the information itself.

2.10.3 Organisations should ensure that personal data gathered through a website is transmitted and stored securely.

2.10.4 As a general rule, personal data that is not already in the public domain should not be placed on Web pages without the consent of the data subject. It may be simpler to provide an opt-out mechanism for data subjects who do not wish their personal details to be publicly available on the Web. This includes employees or members, whose consent should be sought before publicising personal email addresses on corporate websites, unless the organisation's intentions have been made clear in conditions of employment or membership. Note that although placing personal data on a website counts as processing by the organisation, it may not count as export by that organisation for the purposes of Principle 8. It may, however, be export by the internet service provider so caution is required.

2.11 Data sharing

2.11.1 The Act does not provide a power for organisations to share personal data and another basis in law is required for data sharing to comply with Principle 1. This can be either specific legislation or an implied power to share data derived from the function of the bodies, which should suffice for a condition in Schedule 2 to be found. Organisations proposing to share personal data should establish a lawful basis for data sharing.

2.11.2 Data sharing will be in breach of Principle 2 unless it can be shown to be processing compatible with the purpose for which it was obtained as well as lawful. There are, however, limited exceptions to the "non-disclosure provisions" in Part II of the Act which provide gateways to data sharing.

2.11.3 Organisations proposing to share personal data should consider whether a duty of confidence is owed in relation to it. Factors to consider include:

- Whether there is a legal requirement to share the information (e.g. notification of certain diseases)
- Whether the public interest in sharing the information overrides that of withholding it, e.g. if it concerns life-threatening circumstances
- Whether the person concerned has given consent to data being shared
- Whether sharing the data would amount to taking unfair advantage of the person providing it

2.11.4 Another issue is whether data sharing would be in breach of the Human Rights Act and in particular the Article 8 right to a private and family life. To comply with this, data sharing must have a lawful basis and be proportionate. Proportionality involves ensuring that the objective is sufficiently important to justify infringing privacy rights, that sharing is not excessive and that it is being done rationally and fairly.

2.11.5 Protocols setting out the responsibilities and liabilities of all parties should be in place for all instances of data sharing. They should be supported by internal procedures which provide practical guidance to employees. The protocol and procedures combined should ensure that each of the Principles is adequately covered.

2.11.6 Guidance on data sharing is available on the Ministry of Justice's website at http://www.justice.gov.uk/guidance/datasharing.htm, and on other websites to which a link is provided there.

3 RESPONSIBILITIES OF RECORDS MANAGERS

The purpose of this chapter is to complement chapter 2 by summarising the particular responsibilities of records managers for personal data held by them. In many cases archivists share these responsibilities and the chapter will be relevant to them also.

3.1 Responsibilities

3.1.1 Personal data is part of an organisation's records and requires management in the same way as other types of records created or held by it. Where the data is held by a public authority it will be subject to the code of practice on records management issued under section 46 of the UK FOI Act or section 61 of the Scottish FOI Act as applicable. It is likely that personal data will be the responsibility of the records manager at some point in its lifecycle. Records managers can thus expect to have a key role in ensuring compliance with the Act and their job descriptions should reflect this responsibility.

3.1.2 If a records manager who provides or arranges a records centre or other records management services is an employee of the organisation, data protection responsibilities will need to be clearly identified and assigned. There are three likely options:

- The creating division retains primary responsibility, with the records manager acting as custodian, in accordance with directions from that division.
- The creating division transfers full responsibility to the records manager. In this case the records manager becomes a "local data manager" (see Annex A)
- The creating division decides to share responsibility with the records managers and they take joint responsibility for compliance

3.1.3 If a records manager is not an employee of the data controller but provides a records centre or other records management service that the controller purchases, he will be a data processor and must have a written contract that defines how personal data are to be processed (Schedule I Part II, paragraph 12).

3.1.4 Records managers who are themselves obtaining personal information directly from data subjects should ensure that their method of collection complies with guidance at 2.2

3.2 Acquisition and processing of personal data (Principles 1 and 2)

3.2.1 Records managers should be aware of the basis on which personal data and sensitive personal data for which they become responsible was obtained so that they can be confident that their own processing of the data complies with Principles 1 and 2. In practice it may be difficult to establish this for data obtained before the Act came into operation in 2000, although efforts should be made. Data collection from 2000 should have been in accordance with the guidance outlined in chapter 2 and the necessary information should be able to accompany records transferred to the records manager.

3.2.2 Records managers should ensure that all personal data for which they are responsible is processed only for the purpose(s) for which it was obtained or for compatible purposes unless data subjects have given consent to the different purposes (Principle 2). For example, data collected for research purposes should not be used for direct marketing. In practice, records managers may find it difficult to monitor the purposes for which data is being used and should refer users to the corporate data protection policy. See also 4.11.

3.2.3 Some personal data may benefit from the transitional provisions set out at Annex B, B5. However, records managers should weigh the benefits of this against the complexity of applying two regimes to data that is essentially similar in purpose and content.

3.3 Records management policies, procedures and systems

3.3.1 Records managers should ensure that records management policies and procedures are compatible with the Act. If such policies and procedures are not already in place they should be developed and other elements of an effective records management programme should be introduced, in particular retention or disposal schedules specifying how long particular types of personal data will be kept.

3.3.2 Storage facilities and retrieval and access procedures should ensure that personal data is held securely and access provided on a controlled basis only. Security procedures should comply with the corporate information security policy or accepted external standards (see also 2.8). Procedures for the protection of vital records and for disaster recovery should meet accepted standards.

3.3.3 Contracts with staff and third parties, which may relate to external records storage, data back-up or the destruction of confidential waste, should ensure that environmental control, disaster planning and security are covered adequately.

3.3.4 All staff should be aware that the Act applies to data held by individuals, such as personal mailboxes and word processed documents, as well as to data in the corporate records system. Personal filing systems should be discouraged for data that relates to corporate functions so as to reduce the risk to the organisation. Staff in bodies subject to the FOI Acts should be aware that the Data Protection Act applies to all recorded information held by the body, including personal data in manual records that are not part of a relevant filing system, although for wholly unstructured manual data the effect is limited to provision of subject rights of access and correction.

3.3.5 Corporate retention or disposal policies and schedules should ensure that personal data is not held longer than necessary. As a general rule, personal data should be disposed of as a result of the routine application of retention schedules and not on an ad hoc basis. These schedules may provide for personal data to be further processed and kept indefinitely as archives for research purposes.

3.3.6 Electronic document and electronic records management systems should enable access controls to be set so that access to personal data, and in particular sensitive personal data, can be limited. Audit trails of access should be maintained. File and folder titles should include personal names only where this is necessary for retrieval of information. It should be possible to apply disposal schedules so as to delete data no longer required for business or archival purposes.

3.4 Records centre operations

3.4.1 Records centre operations should be compatible with the Act. Staff procedure manuals and user guides should include guidance on data protection matters and provide the necessary instructions.

3.4.2 Transfer arrangements for manual records should ensure quality control. At the point of transfer all key information about the data should be checked to verify record classification, retention periods, access policy and the identification of vital records. The purpose for which the information was obtained and what those contributing it were told should also be checked – essentially the information set out at 2.2.

3.4.3 Any electronic records transferred to the records centre or to an internal or external server should be accompanied by the necessary metadata and treated in the same way.

3.4.4 Arrangements for the transfer of records to an external storage contractor or to an archives repository should be compatible with the Act and, in the case of an external storage contractor, covered by a written contract. Records of all such transfers should be kept.

3.4.5 Retrieval and return arrangements for manual records should ensure appropriate security. This includes keeping authorised user lists up to date and keeping an audit trail of transactions, including all oral disclosures. Electronic records should be treated in the same way.

3.4.6 Procedures for the disposal of records should ensure timely and accurate destruction. Where practicable, manual records should be boxed according to destruction date so that they can be disposed of at box level. Electronic data should be deleted in a way that prevents its reconstruction and security copies, back-ups and other copies of the data should be destroyed also (see also 2.8.3). All disposals should be treated as confidential waste and audit trails of all disposal should be kept

3.5 Inventory of personal data systems

3.5.1 Records managers should ensure that they have access to the inventory of discrete sets of personal data held by the organisation (see 2.6). This is so that they can update it to reflect transfer to the records manager's control and any disposal action after transfer. This will enable the organisation's notification to remain accurate.

3.5.2 Records managers should also ensure that the inventory includes personal data they themselves collect, such as visitor books, authorised user lists, personnel files or customer surveys.

3.6 Notification

3.6.1 The data controller is responsible for notification but records managers should ensure that any discrete sets of personal data collected by them are covered by the organisation's notification. For general guidance on notification see 2.3.

3.7 Maintaining accuracy of personal data (Principle 4)

3.7.1 General responsibilities for maintaining accuracy are set out at 2.4 above. Records managers should take reasonable steps to ensure that the personal data for which they are responsible is accurate and kept up-to-date although not if this would result in loss of superseded information that remains relevant, for example a previous address to which important communications had been sent. It should not be necessary to keep up-to-date any data that has passed out of operational use but if the data subject makes a request for amendment, consider adding or linking a note of the correct information, or a note that the data subject has challenged the information and in what respect. Records managers should keep a record of when updating or correction of data ceased so that its currency can be made known on request.

3.8 Data subject access to personal data (Principle 6)

3.8.1 General guidance on dealing with subject access requests is set out at 2.7 above. Records Managers should ensure that the retrieval of manual and electronic records creates an audit trail. Finding aids must be effective to retrieve personal data quickly and accurately. The data controller should verify and authorise action on all data subject access requests.

3.8.2 The Act provides no rights of access for third parties. Guidance on the circumstances in which third party access can be provided is at 4.9 below.

3.9 Transfer of personal data outside the EEA (Principle 8)

3.9.1 See 2.9 above for guidance on transfer of data outside the EEA.

4 RESPONSIBILITIES OF ARCHIVISTS

The purpose of this chapter is to complement chapter 2 by summarising the particular responsibilities of archivists for personal data held by them. Responsibilities common to records managers and archivists have been described in chapter 3.

4.1 Responsibilities

4.1.1 While ultimate responsibility for compliance with the Act is at the corporate level (see 2.1 above) it is likely that the archivist will play a key role in ensuring organisational compliance with the Act. The archivist, like the records manager (see 3.1), should ensure policies and procedures are compatible with the Act, particularly in relation to storage and access.

4.1.2 Archivists will be concerned with two types of personal data: personal data in their own administrative records, such as staff and reader records and correspondence with depositors, and personal data in the archives within their repository.

4.1.3 Archivists often manage the collections of many different organisations and individuals within their repository, and the nature of the agreement made with the depositor or donor will determine the role of the archivist in relation to each collection. The responsibilities of each party in relation to data protection must be clear.

4.1.4 As a general rule archives received by an archives repository can fall into any of three categories:

- Records transferred from within the organisation, which may be a public authority or a private sector body such as a business. Corporate policy should set out the basis on which archives containing personal data will be passed to the archivist and the level of control and responsibilities that will be passed with them. Like the records manager, the archivist may be acting in a “local data manager” capacity (see Annex A) in relation to transferred records
- Gifts, legacies or purchases, the common factor being that ownership of the archives passes to the archives repository or its parent organisation. The data controller will be the organisation of which the archives repository is a part, with the archivist as “local data manager” unless there is explicit provision to the contrary
- Deposits on loan from external sources, whereby custody passes to the archives repository but ownership remains with the depositor or another party, such as a Trust. In such

cases the organisation of which the archives repository is a part may become sole data controller or may share that responsibility with the owner as joint data controllers, or may act merely as a data processor, leaving control wholly in the hands of the owner. Which applies will depend on the terms of the deposit. As a general rule, the more control over access and use passed to the archives repository, the more likely it will be that its parent organisation has acquired data controller responsibilities. A variant of this last option occurs when control passes to the archives repository in whole or in part, but storage is contracted out to a third party which is a data processor. What is vital is that the owner's continuing interest in the records and the obligations of all parties are set out clearly in the deposit agreement. If the terms of deposit are unclear and the current owner is unknown or cannot be contacted, the organisation of which the archives repository is a part should be regarded as data controller by default

4.1.5 Given the large number of individuals commonly featuring in archive collections, archivists will not be in a position to ascertain whether they are still alive and hence protected by the Act. If it is not known whether a data subject is alive or dead, the following working assumptions can be used:

- Assume a lifespan of 100 years
- If the age of an adult data subject is not known, assume that he was 16 at the time of the records
- If the age of a child data subject is not known, assume he was less than 1 at the time of the records

4.1.6 When researchers obtain copies of personal data from an archives repository they become the data controllers in respect of those copies and must observe the data protection principles, unless they can claim an exemption, for example because their processing is for domestic purposes only, i.e. personal, family or household use. However, archivists cannot control subsequent use of personal data and it is advisable to assume that researchers will be subject to the Act and make them aware of their responsibilities.

4.2 Acquisition and processing of personal data (Principles 1 and 2)

4.2.1 According to Principle 2, personal data should only be collected for one or more specified lawful purposes and further processing should be compatible with those purposes. As a general rule, processing for the purposes of archival preservation can be

considered a compatible further use of the data and the special purpose set out at 2.3.7 will apply.

4.2.2 Processing for the purposes of archival preservation is undertaken by reference to the "research exemptions" set out in section 33 of the Act (outlined in Annex B, B4). Personal data may be stored indefinitely as archives for research purposes provided that the "relevant conditions" are observed, namely:

- The data is not processed to support measures or decisions relating to particular individuals, and
- The data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject

The meaning of "substantial damage and distress" is discussed further at 4.9

4.2.3 When personal data categories (a)-(d) are being processed in accordance with these conditions, there is also an exemption from Principle 5 but the other Principles must be observed unless the personal data is "eligible data", (see Annex A), in which case further exemptions apply (see Annex B). The data may be disclosed to third parties for research purposes in accordance with section 33 or to the data subject without the exemption from Principle 5 being lost. (See also 4.9.) Category (e) personal data is exempted from Principles 1-3, 5, 7 and 8. (See Annex A for an explanation of the different categories of personal data.)

4.2.4 All archives repositories acquiring personal data falling into categories (a) to (d) and wishing to undertake further processing must be able to show that there is a "fair" and "lawful" basis for doing so, in accordance with Principle 1 (See 2.2.5–2.2.6). This means looking at the conditions in Schedule 2 and, for sensitive personal data, Schedule 3.

4.2.5 For schedule 2, archivists dealing with public records will be exercising statutory functions under the Public Records Act and so can refer to paragraph 5(b), which relates to processing for the 'exercise of functions … conferred by an enactment'. Archivists dealing with other public sector records can refer to paragraph 3, which relates to processing 'in compliance with any legal obligation' (other than a contract), paragraph 5(c) which relates to processing for 'the exercise of any functions of … a government department' or paragraph 5(d) which relates to processing for 'functions of a public nature exercised in the public interest'. Archivists in the private sector can refer to paragraph 5(d) also, particularly if the organisation admits

visitors seeking to undertake research. Another possibility for private sector archivists is paragraph 6(1), which relates to processing that is necessary 'for the purposes of the legitimate interests of the data controller' or by third parties to whom the data is disclosed, except where processing would be unwarranted because of 'prejudice to the rights and freedoms or legitimate interests of the data subjects'.

4.2.6 One of the conditions in Schedule 3 must also be identified for sensitive personal data. Archivists processing sensitive personal data who are unable to comply with any of the conditions specified in Schedule 3 may benefit from SI 2000 No. 417 Data Protection (Processing of Sensitive Personal Data) Order 2000. This sets out additional circumstances in which sensitive personal data may be processed and thereby provides supplementary Schedule 3 conditions. Paragraph 9 of the Order makes lawful any processing which, in addition to satisfying the general requirements that sensitive data are processed lawfully and fairly:

"(a) is in the substantial public interest;
(b) is necessary for "research purposes" (which expression shall have the same meaning as in section 33 of the Act);
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
(d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person."

4.2.7 Except when they themselves collect data for the purposes of administering their offices, archivists will generally not be expected to inform data subjects of processing they undertake for research purposes because to do so would involve disproportionate effort. The unfairness of not so informing data subjects is minimal where the relevant conditions are observed and records either kept closed for an appropriate period or used only for research which will be anonymised.

4.3 Appraisal (Principle 5)

4.3.1 Archivists involved in the appraisal of records prior to their transfer should ensure that personal data worthy of permanent preservation is identified as soon after creation as possible and scheduled for retention accordingly (Principle 5).

4.3.2 There is a danger that over-cautious interpretation of the Act may lead to the weeding, anonymising or destruction of files containing personal data that would otherwise be passed to the

archives repository. An archivist's ability within the Act permanently to retain personal and sensitive personal data for the purposes of research (see 4.2.1) should therefore be made clear to potential depositors. The legislation contains the necessary safeguards for depositors.

4.3.3 When considering the permanent preservation of sensitive personal data for the purposes of research, archivists should give serious consideration to how far this will be in "the substantial public interest". This will mean weighing up whether society as a whole, and the research community in particular, will benefit from preservation of the data for research purposes. All appraisal decisions should be documented as a matter of good professional practice.

4.4 Accessioning

4.4.1 All newly received archives, whether manual or electronic, should be checked to ascertain whether they include personal data covered by the Act, for example a database or a series of case files about named living individuals. Bodies that are not subject to the FOI Acts will find that some manual archives fall outside the Act because they are neither accessible records (category (d) personal data) nor records from a relevant filing system (category (c) personal data).

4.4.2 Bodies subject to the FOI Act should assume that all archives containing personal data about identifiable living individuals are subject to the Act. Archivists in public authorities should note that category (e) personal data in archive collections of private origin may fall within the Act by virtue of being held by a body subject to the UK FOI Act[4]. The position is different for bodies subject to the Scottish FOI Act; personal data of private origin will fall within the scope of the Act only if ownership has passed to the archive repository or its parent body.

4.4.3 When arranging the transfer of archives, archivists should ascertain from the donor or depositor whether they contain data already covered by a notification, whether the data is already exempt from subject access and whether measures have been taken to confirm its accuracy. Transfer documentation should incorporate questions that confirm these points (see examples at Annex C).

[4] Assessment of private archive collections to determine whether they fall under the FOI Act is the subject of guidance issued by The National Archives in 2005 - see http://www.nationalarchives.gov.uk/documents/guidance_private_archives.pdf

4.4.4 Transfer and deposit agreements should clarify the responsibilities of the archivist, stating whether the originating person or body is retaining or transferring data controller responsibilities as outlined at 4.1.3. It may be necessary to obtain legal advice to ensure that the wording of these agreements is accurate.

4.4.5 As a general rule, it is simpler to accept only those sets of personal data that are no longer required for current business and hence can be retained for the sole purpose of archival preservation. This is because it will be clear that they are a contemporary not up to date record. However, this may not always be practicable and continued use may prove necessary (see 4.11 for further guidance on this). Notification should accommodate expected use of the data. It should also be clear to someone consulting the data whether the records are still in active use and have been kept up-to-date, or instead reflect a historical position.

4.5 Inventory of personal data systems

4.5.1 As with current and semi-current records, archivists should be aware of collections of personal data held by them, either within the archives or as part of internal administrative records. Administrative records are likely to include files concerning users, such as applications for access; search room attendance registers; logs of virtual visitors; permissions forms, and copyright declarations. Donor and acquisitions files, correspondence, and staff files should also be considered in the audit.

4.5.2 A comprehensive audit of personal data held in the archives, in both manual and electronic form, should be carried out (see 3.5 above). This will enable identification of archives subject to the Act and imposition of handling etc conditions required to ensure they benefit from the research exemptions outlined at 4.2.

4.5.3 Bodies that are subject to the FOI Act should also include category (e) personal data in the audit in order to identify archives that, while not within a relevant filing system, are nonetheless relatively structured as opposed to wholly unstructured (see Annex A). While all category (e) data is exempt from Principles 1-3, 5, 7 and 8, wholly unstructured data also benefits from reduced subject access requirements – see 2.7.3 above and see Annex B.

4.5.4 The majority of manual records held by archives offices will not be sufficiently structured to form part of “relevant filing systems” but will be either relatively structured or wholly unstructured.

Here are some examples of archives with suggestions for the category into which they are likely to fall:

• Council or Board minutes	Unstructured if no name indexes are available; relatively structured if names are indexed to the relevant meeting; structured if indexes are specific to the type of information and its location in the minutes
• Admission/discharge registers to hospitals	Unstructured
• Patient records / case notes	Relatively structured
• Missionary candidates papers	Relatively structured
• School admission and punishment registers	Unstructured
• Personnel files	Relatively structured or relevant filing system, depending on the internal structure of the files. If they are organised so that specific information about individuals is accessible, either through an internal breakdown of types of document within the file or some form of tagging, it is likely to count as part of a relevant filing system. Otherwise it is likely to count as relatively structured. (See Annex B for particular exemptions applying to some personnel files.)
• Adoption and other case files	Relatively structured

4.6 Notification

4.6.1 Archivists should ensure that the archives are included in their organisation's notification as necessary (see 2.3 for details).

4.7 Maintaining accuracy of personal data (Principle 4)

4.7.1 See 2.4 above for general guidance on maintaining accuracy. However, personal data preserved as archives are not expected to be kept “up-to-date” in the same way as data still subject to operational use. Archives are concerned with historical integrity rather than current accuracy. It seems likely that in the event of legal proceedings being brought under section 12A or section 14 by a data subject over inaccuracy, the court would order data to be supplemented by a statement of the true facts rather than replaced. Archivists should be able to rely on the use of supplementary statements or certificates to make the rectification without damaging archival integrity.

4.7.2 If, however, data continues to be used for business purposes as set out in 4.11, requests from data subjects for the correction of data may have to be met. A record of such corrections, and of the original data, should be kept so as to enable historical research to be based on contemporary not current information.

4.7.3 A greater threat to the integrity of archival collections is posed by the right of data subjects to block, erase or order the destruction of personal data they believe to be false (section 12A and section 14). This applies to all categories of personal data. Schedule 8 provides an indefinite exemption from section 14(1) to (3) (but not from the remainder of section 14) for eligible manual data processed only for historical research in accordance with the conditions set out at section 33(1). Other categories of manual data are subject to section 14 in full or, in some cases, the transitional arrangements provided by section 12A until 23 October 2007, and thereafter to section 14 in full. However, in the event of an individual taking action through the courts to secure destruction, and the Information Commissioner’s views being sought, he would not expect to support destruction of personal data selected for permanent preservation as archives.

4.8 Data subject access to personal data (Principle 6)

4.8.1 Archivists who are data controllers (or joint data controllers) will be responsible for providing data subject access to personal data covered by the Act. General guidance on dealing with subject access requests is set out at 2.7 above.

4.8.2 Although archivists may find they have no legal obligation to respond to a data subject access request, for example when the records concerned are held for archival preservation purposes

only and are not open for research (section 33(4)), it is nonetheless good practice to consider providing the data as a matter of policy, especially if the rights and entitlements of individuals are at stake. The exception to this is information exempt from data subject access under Part IV of the Act where provision of access could undermine the purposes of processing, e.g. personal data being processed for the purpose of prevention or detection of crime (section 29). If the section 33 exemption applies, but access is being provided to the data subject as a matter of policy, then the cap on fees set out at 2.7.2 does not apply.

4.9 Third party access to personal data

4.9.1 The Freedom of Information Acts have made significant changes to provision of third party access where bodies subject to those Acts are concerned. The text that follows deals first with access in accordance with the Data Protection Act (4.9.2 - 4.9.6) and then with the effect of the FOI Acts on access to personal data (4.9.7 - 4.9.12).

Access in accordance with the Data Protection Act

4.9.2 The Act does not give third parties rights of access to personal data. Access to personal data in archives by someone other than the data subject or the data controller (or his employees) will normally be permitted for historical or statistical research under the *relevant conditions* (see 4.2). Such access will be subject to closure periods up to a maximum of 100 years, the assumed lifetime of the individual. In administering shorter closure periods or otherwise authorising disclosure of data, archivists should be able to cite conditions in Schedules 2 and 3 as applicable and should consider the following two criteria:

4.9.3 (a) Access must be lawful
Principle 1 requires data to be processed lawfully and so, even if the Act seems to provide no impediment to access, other aspects of lawfulness must be considered:

- Statutes protecting the confidentiality of personal information must be respected. For example, the Sexual Offences (Amendment) Act 1992 protects the identity of victims and alleged perpetrators of rape and some other sexual offences during their lifetime. Archivists should check whether any statutory bars to access apply to personal data they propose to release. The former Department for Constitutional Affairs published a report which identifies the main statutory bars

that apply.[5] It can be seen at http://www.foi.gov.uk/reference/ReviewOfStatBars.htm .

- A duty of confidence may attach to particular records, such as health records, where the consent of the individual is required unless there is an overriding public interest in disclosure. This will necessitate consideration of the way in which the information was first acquired, its nature and age (see 4.9.4), and whether research will make possible the identification of individuals
- The information made available must not be libellous or obscene
- If the information is held by a public body, the Human Rights Act may make access impossible (see 4.9.12)

4.9.4 (b) Access must be fair

Principle 1 also requires data to be processed fairly. Fairness to people about whom personal data are held is the overriding concern of the Act and the guiding principle is when in doubt, withhold the data. The impact of disclosure, including whether it would cause substantial damage or substantial distress, should be assessed, taking into account the following factors:

- The nature of the information must be considered. Some personal information, including some "sensitive personal data", is comparatively innocuous, some is not. To take medical information as an example: information about hospitalisation for a broken leg 20 years ago is not something people feel a need to keep secret whereas information about treatment for a mental illness 40 years ago is still considered to carry a stigma and hence is not for disclosure. In both cases the information is "sensitive personal data" under the Act but different judgements as to whether substantial damage or distress are likely to be caused by disclosure can be formed. Another example, not relating to "sensitive personal data", is information about receipt of public funds. When the funds are received as of right (such as the old age pension or housing repair grants) there are no implications about the income of recipients and hence it is unlikely to be considered embarrassing, whereas when the funds depend on means testing (such as supplementary pensions or social fund payments) receipt is associated with low income and disclosure could be regarded as invasion of privacy and hence unfair to the individual.
- The age of the information may be relevant. The need to provide protection diminishes over time. For example,

[5] The report deals with statutory bars within UK legislation. Some of them may apply to information held by Scottish public authorities but any Order under the UK Act to repeal or amend these statutory bars can apply only to bodies subject to that Act. Note that the review did not look at statutory bars in legislation passed by the Scottish Parliament.

membership of an extreme political group or party may be of little interest after 20 years and none after 40 and disclosure therefore may not damage the data subject's reputation or standing in the community. The age and status of the data subject should also be considered as this can affect the extent of distress they might feel.

- Genuine information (as opposed to speculation) already in the public domain because it is a matter of public record should normally be accessible. An example would be conviction for an offence in a court where no restrictions on naming the person apply (although note that a court case file may contain a mixture of information placed in the public domain at the time of the trial and information that was not made public). Potentially distressing information deliberately made public by the data subject should also be made accessible
- The credibility of the data, i.e. its likely accuracy and comprehensiveness, should be considered as this affects whether the good name of the individual is likely to be put at risk by disclosure
- It is impossible to anticipate what research may be done on any particular set of data but, if substantial damage or substantial distress to any individual would be a likely consequence of any research, the data should remain closed. (Note that processing for medical purposes and racial equality monitoring is allowed, see Schedule 3, paragraphs 8-9)

4.9.5 Steps to safeguard the fair and lawful use of data include:

- Explaining to intending researchers the "relevant conditions" that apply to the research use of particular data, including sensitive personal data (see 4.2)
- Requiring researchers to sign a declaration that, as a condition of access to data that might otherwise be closed, they will comply with the relevant conditions and Data Protection Principles (1, 3-4 and 6-8). Application forms to consult specific personal data subject to these conditions should be signed and kept as an audit trail
- Informing researchers that they are responsible under the Act for any processing by them of personal data disclosed to them, including copying, realignment, transmission abroad and publication (see 4.1.6)
- If researchers are bound by a sectoral code of practice or particular employer requirements, e.g. guidelines produced by a university ethics committee, making access conditional on the researcher undertaking to comply with that as well as with any special conditions applying to specific sets of personal data. This is particularly relevant if he intends to

publish or to make use of the data for purposes other than private research

4.9.6 Note that if researchers breach the terms of any access conditions and publish name-identifiable information, the exemption from section 7 will be lost but not the general exemption for processing for research purposes.

The effect of the FOI Acts on access

4.9.7 If personal data is in archives that are subject to FOI, i.e. they are held by or on behalf of a public authority, then the position is rather different. Third parties seeking access to personal data subject to the Act have the right (i) to be told whether it is held and (ii) to be provided with it, unless an exemption applies. There is a presumption that information provided to an enquirer under FOI is available to any other enquirer, i.e. access to one means access to all.

4.9.8 The most relevant exemption in the UK Act is at section 40 and in the Scottish Act at section 38. It requires archivists to consider whether confirming the existence of the data or releasing it would breach any of the Principles. For categories (a)-(d) personal data it also requires consideration of whether such confirmation or disclosure would breach a data subject's right to prevent processing likely to cause damage or distress (section 10). If so, the exemption should be applied. In practical terms this means considering the factors at 4.9.3 and 4.9.4 as before. However, note that it is not possible when providing access under the FOI Act to impose any conditions on access to, or use of, personal data covered by the Act.

4.9.9 If the section 40 or section 38 exemption is being applied because the personal data should not made generally accessible, one option is to refuse access under FOI and then grant access outside FOI, under section 33 of the Data Protection Act, protecting the data subjects by imposing conditions on access and use as suggested at 4.9.5. In such circumstances it is important that researchers understand that access is being refused under FOI and instead is being granted in accordance with the Data Protection Act.

4.9.10 The section 40 and section 38 exemptions can also be applied if data subject access rights do not apply, i.e. the data is covered by an exemption in Part IV of the Act. See also 2.6 and 4.8.2 above.

4.9.11 If the personal data requested is environmental in nature, the 2004 UK Environmental Information Regulations and

Environmental Information (Scotland) Regulations make equivalent provision at Regulations 13 and 11 respectively.

4.9.12 Note that even when provision of access is not prevented by the Act, other FOI exemptions may need to be considered also. For example, the exemption at section 38 of the UK FOI Act and section 39 of the Scottish FOI Act, which allows information to be withheld if release would endanger the physical or mental health or the safety of a living individual, or the exemption at section 41 of the UK Act and section 36 of the Scottish Act for information to which a duty of confidence is owed, may apply.

4.9.13 Another aspect to consider is whether providing access under FOI could breach the Human Rights Act 1998. This Act gives living individuals the right to respect for private and family life. The impact of disclosure of personal data on the lives of the data subject and family members should also be assessed therefore.

4.9.14 Decisions to allow or refuse access should be explained and documented so that archivists can demonstrate that they have acted in accordance with the Act and in good faith. In the case of personal data subject to the FOI Act, the requirements for refusals set out in section 17 of the UK Act and section 16 of the Scottish Act, which include explaining the basis for the refusal, should be considered.

4.10 Finding aids

4.10.1 Electronic finding aids made available to the public are covered by the Data Protection Act 1998 if they include entries containing personal information about identifiable living persons. Manual finding aids will also be covered if they hold personal information in a relevant filing system in such a way that specific information about particular individuals is accessible. An example would be a list structured by name and subject, as in:

> Taylor, Miss Brenda: adoption
> Taylor, Mrs Catherine: child abuse
> Taylor, Mr Tom: incest with daughter

Manual finding aids lacking this structure will also be covered if held by a body that is subject to the FOI Act, but only to the extent that subject rights of access and correction apply.

4.10.2 Provision of public access to lists containing information of this kind should be avoided if individuals are identifiable.

4.10.3 Finding aids should be considered as a whole when assessing their compliance with the Act. Different levels of descriptive text

should be considered together. For example, an item level description may be innocuous in itself but when read in conjunction with the series level information may infringe the individual's data protection rights. On the other hand, an item description may be acceptable because of the additional information provided at other levels, as long as that information is readily accessible.

4.10.3 As a general rule, assessment of the compliance of finding aids requires consideration of the same factors as outlined above for third party access (see 4.9). A number of questions can be asked:

- Is the item open or closed? If the item is closed, consider whether the description reveals the information which closure is designed to protect. If it does, it may be necessary to amend the description or redact it until the item can be released. If absolutely necessary the full description should be withheld it from the public. If the item is open, the description must be open but it must be fair, accurate and unlikely to cause substantial damage or substantial distress (see the last question)
- Is the person alive or dead? Assume a life span of 100 years if you do not know the individual's date of death. See 4.1.5 for other assumptions to use
- Is the person identifiable? In this context, identifiable means not only identifiable from the finding aid itself but also from other information held by the archives repository, including the archives themselves. Note that a name in itself may not make a person identifiable; it is the name's association with other information, such as the position held or an event or location, that will usually enable the individual to be identified. If the document is closed and the description does not provide sufficient information to identify the individual, a personal name can be included in an open description. For example, an item about a criminal trial might be described as "Trial of J Jones for murder" but while the item is closed, J Jones is not identifiable from the finding aid itself
- Is it really necessary to identify the individual in a description? If the archives have been selected because they contain policy or precedent papers, or because they relate to particular types of cases, there is usually no need to include in the description the names of individuals because the focus should be on the policy or precedent or type of case
- Is there a statutory restriction on releasing information in the description? Some other statutes protect the confidentiality of personal information (see 4.9.3). If a name is central to the reason for selecting the file and should therefore be in the description, the description should be withheld or

redacted while the document is closed. If a name need not be included in the description (because, for example, the file deals with a precedent) and there are no other reasons why the description should not be released, then the description can be open

- Is the information in the public domain already? Information disclosed in open court is in the public domain unless it is clear that reporting restrictions have been imposed and not lifted. Cases heard in camera are not in the public domain
- Is the description accurate? Occasionally contemporary information is subsequently found to be inaccurate. The information must be fair to the living individual, while conveying the information in the contemporary record
- Is the description unambiguous so that there is no doubt about the good name of the individual? If, for instance, the item relates to criminal proceedings it may be possible to ascertain from it or a related record whether the individual was convicted or acquitted; if not, the description should be worded in such a way as to make it clear that inclusion in the finding aids is not evidence of guilt.
- Is it likely that release of personal information in a description could cause substantial distress or substantial damage to the data subject? This applies particularly but not exclusively to sensitive personal data. It is necessary to exercise judgement to assess the severity of distress or damage that might be caused. See 4.9.4 for examples.

4.10.4 Bodies subject to the FOI Acts may receive a request for information in a closed description, often as a precursor to a request for the information itself. While there is a duty to confirm or deny that information is held and to provide that information, an exemption from that duty can be claimed if to do so would amount to releasing exempt information. Decisions on whether or not to release closed descriptions should be made on the same basis as decisions on the information itself, for which see 4.9.

4.11 Business use of archived data

4.11.1 The wording of Principle 2 makes it clear that data can lawfully be used for more than one purpose at a time. An organisation collecting information for business purposes can continue to use data in its archives for these business purposes as long as the use is otherwise fair and lawful and the appropriate notification is in place (see also 4.2.1).

4.11.2 It is possible that depositing organisations will seek to use data held in an archives repository for purposes of current business

that are not covered by its current notification. Where the depositing organisation considers such use is likely to take place, the original purpose for processing must continue to be notified to the Information Commissioner, along with the new archives purpose (for which see 2.3.7). So, for example, if a grant-giving body removes from its current records system to its archives some files about old research grants, but expects to need to refer to those files some time in the future, e.g. in order to deal with an application for a further grant from the same person, the notification should reflect that expected use. When this operational use is no longer expected the notification should be amended to remove the purpose for processing.

4.11.3 In exceptional circumstances there may be a need to use data in the archives for one-off business purposes which are not covered by its current notification. If there is any prospect that this exceptional need will recur, the notification should be amended accordingly. If, however, it is a genuine one-off, processing of personal data will be permissible without amending the notification.

4.11.4 Examples of such one-off situations are:

- The data is being used in its historic context for current planning or decision making
- The processing is being undertaken with the consent of the individual
- The processing is being undertaken in response to a request for action by the data subject. For example, a request that a duplicate war service medal be issued would require verification of entitlement to such a medal, and the request can be taken to include consent to this use of the data. However, if the request for action required use of sensitive data, explicit consent should be obtained from the data subject
- The processing is required for the organisation to defend its legitimate interests. An example is consultation of a file in relation to a complaint or litigation
- It has not been possible to obtain consent but the archivist has reasonable grounds for believing that the processing could be to the benefit of the data subject and that consent would have been given. An example would be disclosure to a solicitor seeking the beneficiaries of a will. In such circumstances an assessment of the effects of disclosure should be undertaken before disclosure and the decision, with the factors considered, documented.

Note that this unexpected processing will still have to comply with the requirements of the Act, such as Principles 1 and 2, regardless of whether notification is required.

4.11.5 Processing other than for archives purposes may be undertaken by data subjects who are using the data for their own purposes. Data subjects do not need to justify their use of personal data about themselves.

4.12 Security of personal data (Principle 7)

4.12.1 Archivists are responsible for the security of personal data in their care and, in accordance with existing professional practices, should ensure that "adequate" levels of security are provided for it. Quite what "adequacy" entails will depend mainly on the nature and age of the information and the extent to which it requires protection. (See 2.8 above for details of measures that should be in place.)

4.13 Transfer of personal data outside the EEA (Principle 8)

4.13.1 See 2.9 above for general advice when considering the transfer of personal data outside the EEA. Archivists should pay particular attention to the following activities that might be caught by Principle 8:

- *Responding to enquiries on living individuals from researchers outside the EEA (e.g. USA, Canada, Australia, New Zealand and African countries)*
  - If the archives are lawfully open for research on an unconditional basis, and hence the decision has already been made that disclosure will have no adverse effect on the data subject, export is considered by the Information Commissioner to fall within Schedule 4, paragraph 8 and is acceptable
  - If the archives are generally closed and made available to researchers only on a conditional basis, e.g. that the results of the research will be anonymised, it may be possible to justify export under Schedule 4, paragraph 8. This will require safeguards to protect the interests of the data subjects, such as ensuring that the researcher has signed a specific undertaking concerning use of the data before the data is despatched

- *Sending personal data overseas for keyboarding, e.g. for retro-conversion of archival catalogues*.
  In this case a contract with the external company undertaking the re-keying should provide a regime that protects privacy

equivalent to the Data Protection Act (see 2.9).

- *Placing digitised copies of archives containing personal data on a website*
  - Archives should not be placed on a website unless their contents have been reviewed, using the criteria set out at 4.9, and it has been concluded that no substantial damage or distress would be caused to data subjects by making the archives available in this way. Placing personal data on a website counts as processing by the archive repository but not as export to a third country, according to the European Court, because it is the internet service provider that is doing the exporting[6]. Archives should never be placed on a website unless they are available for research on an unconditional basis.

4.13.2 Note that, in any event, transfer is permitted if the consent of the data subject has been obtained.

[6] The European Court in the Lindqvist case (C-101/01 of 6 November 2003)

ANNEX A EXPLANATION OF TERMS USED IN THE ACT AND IN THIS CODE

Accessible records
See Personal data

Automatically processed data
See Personal data

Categories (a) – (e) data
See Personal data

Closed record
This is a record that is not available for general public access. Note that it may be possible to provide access to information within the record in response to an FOI request, for example by redacting the record to remove information that should be withheld, such as information identifying individuals. It may also be possible to provide access to those agreeing to specified restrictions on use (see 4.9.5).

Data controller
This is the person (an individual or other legal person such as a company) who determines why, as well as how, personal data are to be processed. It is their duty to ensure that the collection and processing of any personal data within the organisation complies with the requirements of the Data Protection Act.

Data processor
This is any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors must have a written contract in which the data controller defines how personal data, including sensitive personal data, is to be processed and what security measures will be appropriate. Although the data processor must, of course, observe the terms of the contract, the data controller retains full responsibility for the actions of the data processor.

Data subject
The person who is the subject of the personal data. To count as a data subject the person must be living and capable of being identified from the data or other data in or likely to come into the possession of the data controller.

Eligible data
Data – automated or manual - that was subject to processing already under way immediately before 24 October 1998. It includes data added since that date as long as it is of the same type and being subjected to the same type of processing

Eligible manual data

See Eligible data

FOI Acts
Used collectively for the Freedom of Information Act 2000 and the Freedom of Information Act (Scotland) 2002. The Scottish Act applies to bodies that fall under the Scottish Parliament and Scottish Executive or are otherwise identified as falling under it; all other Public authorities fall under the UK Act.

Historical research
Any research done in an archive repository will be “historical” in its widest sense.

Local data manager
For the purposes of this Code, the term “local data manager” is used for the individual within the organisation to whom responsibility for particular sets of data has been delegated. For example, a personnel manager might be “local data manager” for personal data in personnel files and the records manager might be “local data manager” for records transferred to his care.

Manual data in 'relevant filing systems'
See Personal data

Non-disclosure provisions
See Annex B, B3.3

Open record
This is a record that is available for public access on an unconditional basis.

Personal data
Information relating to living individuals who can be identified from that data or from that data and other data in the possession of, or likely to come into the possession of, the Data Controller. It includes expressions of opinion about, and any indications of anyone’s intentions in respect of, that individual.

There are five categories of personal data:

- *Category (a)* Information being processed by means of equipment operating in response to instructions given for that purpose, for example a database or a system with search capabilities which enables information about individuals to be identified and retrieved
- *Category (b)* Information recorded with the intention of being processed in accordance with category (a)
- *Category (c)* Information that is not processed automatically but is recorded as part of a “relevant filing system” or with the intention that it should form part of a relevant filing system. A relevant filing system is one in which particular information about specific individuals can be readily retrieved. The internal structure of the files is therefore relevant. Any system whose primary purpose is to hold information about individuals and comprises files with an

internal structure or referencing system that facilitates retrieval of specific information about those individuals falls within this definition.

- *Category (d)* Records relating to health, education, social work and housing that were previously subject to an equivalent right of data subject access under other legislation. There is a statutory definition at section 68.
- *Category (e)* Recorded personal information that does not fall into any of the above categories and is held by a public authority as defined by the FOI Acts. This category divides into two sub-categories:
    - ***Relatively structured data***. This is data that is part of, or is intended to be part of, a set of information relating to individuals and that is structured by reference to individuals or by criteria relating to individuals but that does not have an internal structure or referencing system that would facilitate retrieval of specific information about particular individuals. An example would be a set of case files with a chronological arrangement of papers within each file and which was not otherwise indexed.
    - ***Unstructured data***. This is data that does not have the type of structure described above. An example would be a policy or subject file in which details of an individual occurred randomly.

Processing
This has a very wide meaning. Passively holding information counts as processing as well as actively obtaining, recording, using, amending or destroying it.

Public authority
A body covered by one of the FOI Acts. Note that the amendments to the Data Protection Act in the UK FOI Act that apply only to public authorities were extended to Scottish public authorities by the Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004.

Relevant filing system
See Personal data

Scottish FOI Act
The Freedom of Information (Scotland) Act 2002

Sensitive personal data
Personal data consisting of information about:

- Someone's racial or ethnic origin
- His political opinions
- His religious beliefs or other beliefs of a similar nature
- His trade union membership
- His physical or mental health or condition

- His sexual life
- The commission or alleged commission of offences by him
- Details of any proceedings for any offence committed or alleged to have been committed by him, and the outcome of such proceedings including the verdict and, if applicable, the sentence

Subject information provisions
See Annex B, B3.2

Unstructured manual data
See Personal data

ANNEX B OVERVIEW OF THE ACT

B1 Data Protection Principles

B1.1 The eight Data Protection Principles (the Principles) form the basis of the Act and must be observed, even if the processing of the data is exempt from notification. The Principles as set out in Part I of Schedule 1 to the Act are:

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 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 those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

B1.2 Guidance on interpreting these Principles is at Part II of Schedule 1.

B2 Enforcement

B2.1 The Information Commissioner enforces the Act by issuing enforcement notices. Data subjects have the option to ask the Information Commissioner to enforce the Principles rather than going to court. Failure to comply with an enforcement notice is a criminal offence (sections 40-47, 60).

B2.2 Other offences created by the Act include processing electronic data without due notification (sections 21-22) and knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller (section 55).

B2.3 Individual officers whose knowledge, connivance or neglect contributes to an offence committed by a corporate body are also guilty of the offence; on conviction offenders are liable to a fine (section 61)

B2.4 Individual officers in public authorities commit an offence if they alter, deface, destroy or conceal a record containing information to which section 7 gives a right of access with the intention of preventing disclosure of the requested information; on conviction offenders are liable to a fine (FOI Act, section 77).

B2.5 Appeals against the Commissioner's notices may be made to the Information Tribunal and, for appeals on points of law only, from the Tribunal to the High Court (sections 48-49).

B2.6 Note that although government departments cannot be prosecuted under the Act, a civil servant can be prosecuted for obtaining or disclosing data in breach of section 55 (section 63) or for altering etc data as described at B2.4.

B2.7 The Information Commissioner enforces the UK FOI Act but a separate Scottish Information Commissioner enforces the Scottish FOI Act.

B3 Rights of data subjects

B3.1 Part II of the Act sets out the strengthened rights of data subjects in relation to processing:

- Schedule 1, Part II, paragraph 2 obliges the data controller (when obtaining data) to tell the data subject the identity of the data controller and the purpose of processing. If the data was not obtained from the data subject, the information is to be given as soon as practicable unless provision of the

information would require disproportionate effort or the data controller is required to record or disclose the information by a legal obligation other than a contract. Archivists receiving records relating to thousands of individuals are not expected to contact each data subject because this would involve disproportionate effort.

- Sections 7-9 cover the data subject's rights of access to personal data. Data subjects have the right to be informed - upon written request and payment of a fee - of the data held, the purposes for which it is to be processed, to whom it will be disclosed and its source. The data controller has 40 days to comply. The information must be intelligible and conveyed in "permanent form" by way of a copy unless the supply of such a copy is not possible, involves disproportionate effort, or the data subject agrees otherwise. If, for one of these reasons, the data controller does not supply a copy, he must find some other way of supplying the information. If asked, data subjects must provide information required to locate the requested personal data and proof of identity.
- Section 9A (UK FOI Act section 68) extends this right to category (e) data held by Public authorities. However, if the data concerned is unstructured personal data, the data subject must describe the information he is requesting. If the cost of locating and identifying that personal data would exceed a cost limit set in 2004 Fees Regulations (SI 2004 No. 3244), the request can be refused. The cost limit is £600 for central Government bodies (those listed in Part I of Schedule 1 to the UK FOI Act) and £450 for all other bodies
- Unless archivists anonymise all personal data (which would destroy their value and is anyway not practicable), they cannot prevent the possibility of a researcher identifying a data subject in published research. Should this happen, the data will not lose its exemption for research purposes but only its exemption from section 7. In most cases, for example, genealogical research or unfavourable biographical references, the data subject will not be adversely affected (see also 4.9.5).
- Section 10 confers the right to prevent processing likely to cause "substantial damage" or "substantial distress" if such damage or distress is unwarranted. This does not apply to category (e) data. The process requires the data subject to send a notice in writing to the data controller, who must respond within 21 days with either a statement that processing has stopped or will stop, or an explanation of why the notice is considered unjustified.
- Section 11 confers the right to prevent processing for the purposes of direct marketing. This does not apply to category (e) data.

- Section 12 gives the data subject rights in relation to automatic decision making
- Section 13 enables damages to be claimed by data subjects for damage and associated distress resulting from breach of the Act's requirements
- Section 14 allows the data subject to request a court to order correction, erasure, blocking or destruction of data that is inaccurate, false or factually misleading (note that this includes accessible records and eligible manual data until 23 October 2007 (section 12A/Schedule 13) but excludes category (e) data (section 14A/UK FOI Act section 70(3)-(4))

B3.2 *The subject information provisions* (section 27(2)) entitle the data subject to know what data about him is being or has been collected. They consist of section 7 and the fair processing information at Schedule 1 Part II, paragraph 2. The former applies to category (e) data but not the latter.

B3.3 *The non-disclosure provisions* (section 27(3)-(4)) prevent any disclosure of data which would be inconsistent with specified data protection principles. These Principles are Principle 1, apart from compliance with the conditions in Schedules 2 and 3, and Principles 2-5. The non-disclosure provisions also prevent disclosure which would be inconsistent with sections 10 and 14(1)–(3). See B4.2 for details of the principles from which category (e) data is exempt.

B4 Exemptions

B4.1 The exemptions from some or all of the provisions of the Act fall into three broad categories:

- The primary exemptions set out in Part IV of the Act (including exemptions introduced by the UK FOI Act and extended to Scottish bodies by the Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004
- The miscellaneous exemptions set out in Schedule 7
- The exemptions arising from the transitional and indefinite provisions set out in Schedule 8

B4.2 Most of the primary and miscellaneous exemptions will only be relevant to records managers in highly specialised offices who are advised to consult the Act and note against the data the particular conditions which apply. The exemptions likely to affect most records managers and archivists are as follows:

- Research, history and statistics (section 33)

The processing of personal data only for research (including historical or statistical) which does not involve their use either to support measures or decisions with respect to particular individuals or to cause substantial damage or distress to any data subject is considered compatible with the second principle. Where research is the specified purpose, or one of the specified purposes, the data may be kept indefinitely notwithstanding Principle 5. The data is also exempt from section 7 (subject access rights) if the results of the research are anonymised.

- Manual data held by public authorities (section 33A, introduced by section 69 of the UK FOI Act and extended to Scottish public authorities by the Order cited at B4.1 above)
  Manual data that is not within a relevant filing system but is held by a public authority has been brought within the scope of the Act by the FOI Acts. This data must be accurate and data subject rights in section 7 and section 14 must be respected although special provisions apply in relation to data subject access (section 9A/section 69(2) of the UK FOI Act). The data is otherwise exempt from the Principles and the greater part of the Act. However, when deciding whether to disclose such personal data to third parties in response to an FOI request, potential breach of any of the Principles must be considered (section 40(3)(b) of the UK FOI Act and section 38(2)(b) of the Scottish FOI Act)
- A sub-set of this manual data, relating to all aspects of employment in the armed forces, under the Crown or in a public authority (section 33A(2)/section 71 of the UK FOI Act applicable also to Scottish public authorities.
  This manual data is exempt from all data protection principles and Part II, Part III and section 55 of the Act.
- Information available to the public by or under an enactment (section 34)
  This is exempt from the subject information provisions and the non-disclosure provisions, e.g. electoral rolls. The enactments referred to exclude the FOI Act
- Confidential references given by the data controller (Schedule 7, paragraph 1)
  References given in connection with the education or employment of the data subject are exempt from section 7. Note that this exemption does not apply to confidential references received by the data controller.
- Management forecasts and planning (Schedule 7, paragraph 5)
  This is exempt from the subject information provisions to the extent to which their application would prejudice the conduct of business

B4.3 Other primary exemptions that affect records managers in certain specialist offices relate to data, the disclosure of which would prejudice:

- The safeguarding of national security (section 28)
- Combating crime and collecting tax (section 29)
- The work of regulatory authorities, e.g. Ombudsmen (section 31)

B4.4 The Secretary of State has the power to make further exceptions from the subject information provisions in relation to data relating to the data subject's records in the areas of health, education and social work (section 30). Several Orders have been made (see http://www.dca.gov.uk/ccpd/dpsubleg.htm)

B4.5 Other miscellaneous subject information exemptions that will affect records managers in certain specialist offices relate to data:

- The disclosure of which would affect the price of financial instruments underwritten by a corporate finance service (Schedule 7, paragraph 6)
- The disclosure of which would prejudice the combat effectiveness of the armed forces (Schedule 7, paragraph 2)
- That relate to judicial appointments, appointments made by the Crown or a Minister and honours and dignities conferred by the Crown (Schedule 7, paragraphs 3-4)
- That would be subject to confidentiality between lawyers and clients (Schedule 7, paragraph 10)

B4.6 Special exemptions apply to subject access requests concerning examination marks and scripts (Schedule 7, paragraphs 8-9).

B5 Transitional provisions and indefinite exemptions

B5.1 General

B5.1.1 The transitional relief from immediate compliance with certain provisions of the Act[7] applies only to eligible data, i.e. to data that was subject to processing which was already under way immediately before 24 October 1998 (see Annex A for an explanation of this and other terms). Processing of data that does not meet this criterion must comply with the Act. Note that adding new data to an existing system is not new processing; if

[7] See Schedule 8 for details. But see also 4.4.2.

the same type of processing was being carried out before the date, the processing is considered to be under way on that date.

B5.1.2 The first timed period of relief ended on 23 October 2001; the second extends to 23 October 2007 and its provisions are summarised at B5.2 below. In addition, there are indefinite exemptions summarised at B5.3 below.

B5.2 Exemptions to 23 October 2007

- Processing other than for historical research purposes

Schedule 8, paragraph 14 applies to eligible manual data and accessible records. The data is exempt, until 23 October 2007, from Principle 1 with the exception of the duty to inform the data subject of the purpose of processing and the identity of the data controller (Schedule 1 Part II, paragraph 2). This duty is to be carried out so far as is practicable and may not be reasonably practicable for most archivists in connection with data within the archives, but each case will need to be considered on its own facts. Eligible manual data and accessible records are also exempt from Principles 2-5 and section 14(1)-(3).

- Category (e) data

Schedule 8, paragraph 14A (FOI section 70(3)) exempts category (e) data from Principle 4 and section 14(1)-(3), in addition to the indefinite exemptions at B4.2 above.

This means that, for categories (a) to (d) personal data, the data controller must ensure compliance with the following parts of the Act:

- Principle 1 (Schedule 1 Part II, paragraph 2) which relates to giving the data subject certain information
- Principle 6 which relates to data subject rights
- Principle 7 which imposes standards of security
- Principle 8 which limits the transfer of personal data outside the EEA
- Part II of the Act (Individuals' Rights) except section 14(1)-(3)
- Part III of the Act (Notification)

And for category (e) personal data he must ensure compliance with:

- Principle 6, modified as set out in section 9A
- Section 14(4)-(6)

B5.3 Permanent (or indefinite) exemptions from 24 October 2001 for historical research

The exemptions set out below apply when processing is for historical research purposes in compliance with the relevant conditions as defined in section 33 (see B4.2 above):

- Eligible manual data

This is subject to the "limited provisions" set out above in B5.2, bullet points 3-8.

- Eligible automated data

If the data are processed by reference to the data subject, the only exemption is from that part of Principle 1 that requires compliance with the conditions in Schedules 2 and 3. If the data is processed otherwise than by reference to the data subject it is subject to the "limited provisions" set out above in B5.2, bullet points 3-8.

ANNEX C SPECIMEN FORMS

1 Personal data report form

2 Data subject access request form

3 Questions to include in a transfer or deposit form or agreement

4 Researcher undertaking concerning access to archives that would otherwise be closed

C1 PERSONAL DATA REPORT FORM

Complete a separate form for each new collection or set of personal information for which you are responsible, whether held electronically or manually in any other medium, e.g. index cards, paper files, microfiche, etc.

1 Business unit responsible for the data	2 Person responsible for the data (name & job title)
3 Name of collection	4 Description of collection & quantity
5 Is it held electronically? If so, & networked, specify folder path & file name. If not networked specify computer	6 Is it held manually? If so, & in a registered file series, specify the series. If not in series, give equivalent identifying details

7 What personal details are included? (tick all that apply)

Name? Postal address? Phone no? Email address?

Date of birth? Nationality? Bank details? Religion?

Health details? Research topic? Trade Union membership?

Other? (please specify)

8 Who provided the information? (tick all that apply)

Data subject? Staff? Other people? (please specify)

9 What is the information used for?	10 What has the data subject been told about its use and disclosure?

11	Do you disclose the information internally? If so, to whom, why, and what do they use it for?
12	Do you disclose the information externally? If so, to whom, why, and what do they use it for? Does it leave the EEA?

13	What are the covering dates of the collection?

14	Is the collection new since 24/10/1998?

15	How accurate is the information? (give an estimate) 50% 70% 80% 90% 100% Don't know

16	What checks were made when it was obtained?

17	Is it on a disposal schedule? If so, what is the disposal action?

18	Who carries out disposal & is it recorded?

19	What are the security arrangements?	(give details for whichever applies)
	For manual files	
	For electronic systems	
	For other current material (please specify)	
	For information no longer required	

20	Other relevant information

Name Date

C2 DATA SUBJECT ACCESS REQUEST FORM

1 Details of person requesting the information

Full name

Address

Tel. No. Fax No

Email address:

2 Are you the data subject?

YES: If you are the data subject please supply evidence of your identity, i.e. original or copy of driving licence, passport, national identity card or photo-pass, and as evidence of address a recent letter or bill from a utility company. Please include a stamped addressed envelope for returning the document
(Please go to question 4)

NO: Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. If not, what other legal justification have you for obtaining access to the data? Please note that identification as above must be provided for you and the data subject.
(Please go to question 3)

3 Details of the data subject (if different from 1)

Full name

Address

Tel. No. Fax No

Email address:

4 Please describe the information you seek together with any other relevant information. This will help to identify the information you require.

We are allowed charge a fee of £10 for each data subject access request. An invoice is enclosed. [USE IF A FEE IS LEVIED; THE FEE IS NOT COMPULSORY]

DECLARATION. To be completed by all applicants. Please note that any attempt to mislead may result in prosecution

1 …….. certify that the information given on this application form to the [ORGANISATION NAME] is true. I understand that it is necessary for the [ORGANISATION NAME] to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data

Signature: Date:

Note. The period of 40 days in which the [ORGANISATION NAME] must respond to the request will not begin until it is satisfied on these matters.

Please return the completed form to the Data Protection Officer, [ORGANISATION NAME AND ADDRESS].

Documents which must accompany this application:

- **Evidence of your identity**
- **Evidence of the data subject's identity (if different from above)**
- **Authorisation from the data subject to act on their behalf (if applicable)**
- **The fee set out on the attached invoice**
- **Stamped addressed envelope for return of proof of identity/authority documents**

C3 ISSUES TO COVER WHEN ARCHIVES ARE BEING DEPOSITED

1 Is the data covered by a notification of processing of personal data under the Data Protection Act 1998? If so, obtain details of the notification.

2 If it is notified, will this notification be continued after deposit to enable retrieval and continued use of the data for business purposes?

3 Does the deposit include any sensitive personal data as defined by the Data Protection Act 1998, section 2? If so, specify the category of sensitive personal data and where it is likely to be found.

4 Who will be data controller for the personal data?
- Is the depositor assigning all data controller responsibilities to the archives repository or
- Is the depositor retaining all data controller responsibilities
- Is the depositor becoming joint data controller with the archives repository

5 If the archives repository is becoming joint data controller, does the depositor want to be consulted by it before data subject access is provided?

6 Do any exemptions from subject access apply? If so, specify the relevant exemption in Part IV that applies

C4 **RESEARCHER UNDERTAKING CONCERNING ACCESS UNDER THE DATA PROTECTION ACT TO ARCHIVES THAT WOULD OTHERWISE BE CLOSED**

I <name> of <address> request permission to consult <archives reference> and agree to make use of any personal data contained therein in compliance with the Data Protection Act 1998. My research will not be used to support measures or decisions with respect to particular individuals and will not cause or be likely to cause substantial damage or substantial distress to any person who is the subject of those data while he or she is alive or likely to be alive (assuming a life span of 100 years).

I will not make the results of my research available in a form that identifies any data subject without the consent in writing of the data subject or the data controller.

I understand that I shall become responsible for compliance with the Data Protection Act 1998 in relation to any processing by me of personal data obtained from the above records and undertake to dispose of this data in an appropriate manner when it is no longer required for my research.

Signed Date

The original signed undertaking should be retained by the archives repository and a copy should be provide to the researcher.

ANNEX D FURTHER READING

The Act and its subordinate legislation

The Act and subordinate legislation are available on the Internet, accessible from
http://www.opsi.gov.uk/legislation/index.htm

Data Protection Act 1998, c.29
http://www.opsi.gov.uk/acts/acts1998/19980029.htm

Freedom of Information Act 2000
http://www.opsi.gov.uk/acts/acts2000/20000036.htm

Freedom of Information (Scotland) Act 2002
http://www.opsi.gov.uk/legislation/scotland/acts2002/20020013.htm

Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004
http://www.opsi.gov.uk/si/si2004/20043089.htm

Subordinate legislation listed on the Ministry of Justice website at http://www.dca.gov.uk/ccpd/dpsubleg.htm under the heading 'Statutory Instruments'.

The Information Commissioner's Guidance

The Information Commissioner's guidance covers most aspects of data protection. Some is available in print, but see the ICO website for up to date guidance:
http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

Other core guidance

BSI BIP 0012, *Data Protection – Guide to the Practical Implementation of the Data Protection Act 1998*
This includes explanations of the provisions of the Act, model forms and templates and a pre-audit workbook. For further details see
http://www.bsi-global.com/ICT/Legal/bip0012.xalter

The Data Protection Act 1998: A Guide for Records Managers and Archivists (Public Record Office, 2000)
http://www.nationalarchives.gov.uk/documents/dpguide.pdf

Records management

Codes of practice on records management under the Freedom of Information Acts
http://www.foi.gov.uk/reference/statCodesOfPractice.htm
http://www.scotland.gov.uk/Resource/Doc/1066/0003775.pdf
These apply only to bodies subject to one of the FOI Acts and, in the case of the UK Act, to bodies that are subject to the Public Records Act 1958.

Data security

BS ISO/IEC 17799, *Code of Practice for Information Security Management* (2005) (also identified as BS 7799-1: 2005)
BS ISO/IEC 27001, *Information technology. Security techniques. Information security management systems. Requirements (2005 forthcoming).* (Also to be identified as BS 7799-2: 2005)