Chapter 2 The laws and regulations

1 Introduction

In this chapter, we will examine the external drivers which influence organisations towards practising good information governance. These are pieces of legislation, regulation and standards which are imposed from outside the organization, and which either must be complied with in order to avoid penalties, or which define benchmarks against which the practices and performance of the organization can be judged.

Sometimes these, in particular the pieces of legislation, are themselves referred to as ‘information governance’, in that they impose rules which govern what organizations do with information. However, as we’ve seen in chapter 1, a more constructive way of understanding the term is to think of ‘information governance’ as those practices which lead to efficient, effective and ethical use of information, the avoidance of legal repercussions being a sign of legislative recognition of the legal correctness of these practices.

The specific laws and regulations dealt with in this chapter will be those which apply in the UK, as space does not permit discussion of equivalent legislation in other legislatures, but it will be found that similar legislation exists in a large number of countries – in March 2013, Rwanda became the 94th country to pass a Right to Information Act (freedominfo.org 2013), the equivalence of EC countries’ data protection laws to those in the UK is discussed in section 4.10 below, as is the list of ‘third’ countries recognized by the EC as having equivalent legislation. Other states, including the twenty-one members of the Asia-Pacific Economic Co-operation Group (APEC) have agreed on privacy principles, and Argentina, Canada, Hong Kong, Israel and Russia have modeled their laws on the European model (Kuner 2010).

The United States has had a Freedom of Information Act since 1966. It applies to records held by federal agencies, such as the Department of Justice and the Department of Health and Human Services, and gives individuals the right to access any agency record, except for those protected from public disclosure for reasons of national security, for example. It also requires the agencies to automatically publish other information, including lists of Frequently Asked Questions and answers to them (FAQs). It is the enquirer's responsibility to determine which agency has the records they require, but all agencies have a web site which lists the types of records they hold. This stance of actively making records available is endorsed as good policy by the UK Information Commissioner's Office, and we shall discuss later why it is a part of a well-thought-out information governance policy.

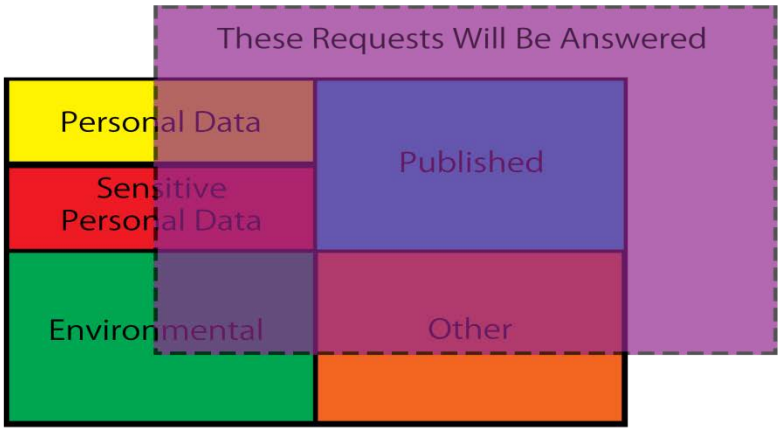

Figure 1 For various reasons, some requests will be exempted from being answered

These laws and regulations are expressions of a relatively new and 'open' attitude to information – that people have the right to know about the activities of, and information held by, public authorities; that giving the public access to environmental information increases public engagement with environmental issues, making public bodies more accountable, and increasing public trust in them.

2 A standard for records

In much of the rest of this book, we'll be discussing records, and what may and may not, what ought and ought not to, be done with them. "[R]ecords are recorded information. Indeed, a record may be defined as *any information captured in reproducible form that is required for conducting business*". (Penn et al 1994 p. 3) As the authors observe, there are different definitions of "information", depending on whether you believe it is raw data, whether it has metadata added, or is data which has been transformed into "knowledge", but the important point is that we need systems for handling it, in order that it may be used in "conducting business" – another expression open to a wide range of interpretation.

As you might expect, there is a lot of recorded information in a university, for example, but not all of it is in the form of records. There is a great deal of recorded information in the library, but, aside from some archival material, which is in the form of records, the library stock is not used, or required, for conducting business. Of course, the library could not operate without stock, and the university could not operate without the library, but the information in the library stock is not required for conducting business. We could exchange one Records Management text for another without any major disruption, but if we transposed personnel records, or student transcripts, or salary records, it does not take

much imagination to see the trouble that might result.

Records have been kept for thousands of years, the media changing from clay tablets to papyrus, from paper to electronic and optical media, but the idea of records management as a function central to the operation of an organisation is of relatively recent origin. Until the period following the Second World War, the "records management" function tended to concentrate on amassing material – the "keep everything" strategy. Whilst this might suffice for limited numbers of records, we have all heard of the "information explosion", and mere accumulation does not enhance usability. There is no value in keeping everything, if you cannot find the item you want, when you want it.

Organisations are under more pressure than ever before to be efficient, and there are also legal requirements to demonstrate efficient and effective records management – The Data Protection Act 1998 and The Freedom of Information Act 2000 are two of the legal instruments enforcing these standards in the UK, but there are equivalent pieces of legislation in many other jurisdictions, and the increase in online activity means that we all have an interest in ensuring that our personal information is safe from abuse, and that we have access to the information which organisations hold about us.

So, there is a competitive advantage to be gained from effective records management, and there is also a requirement to be able to demonstrate good practice in how it is carried out.

2.1 The record life-cycle

One of the post-World War II innovations in records management was the notion that records have a life-cycle – they pass through different stages and types of use, beginning with their creation, moving through a period of active use, then into a semi-active period, and finally to the stage of archiving or disposal. This is also reflected in the ways in which records are managed physically – active records will most likely be found close to those who work with them, perhaps in in- and out-trays on people's desks, perhaps in filing cabinets. Semi-active records will probably be in files, and inactive records will either be disposed of, or may be moved to off-site storage, should they have archival value. Electronic records will undergo a similar process – from "live" files to archives, perhaps written to optical disks, perhaps deleted.

2.2 Costs and benefits

Records, particularly paper records, are a source of costs, relating to their creation, handling, and storage. One of the benefits of a good records management policy is that significant savings can be made in the office space which has been used to store records which need not be there. This can be a major selling point used to convince management of the need for a records management programme, but the fact is that there are many other drivers, which are not so easily measured as the cost per square metre of housing filing cabinets, or the cost per gigabyte of computer disk storage.

The benefits are partly from the absence of things that don't happen if you have a good Records Management policy. Your organisation is able to face an audit with confidence, because invoices and receipts are properly managed. A Freedom of Information request can be handled with ease, because the relevant records are easily traceable. Employees can feel secure that their personal data is handled correctly. Customers can feel secure that their contact and credit card details are not abused. Even the author of a corporate history can trace documents of historical value, in the archives.

2.3 Desirable qualities of records

In order to be authoritative, records ought to possess certain qualities, usually expressed as reliability, authenticity, usability and integrity. Briefly, these can be summarized thus:

Reliability means that the record can be trusted as a full and accurate representation of the activity that it records.

Authenticity means that the record is what it appears to be – that it has been created by authorized and identifiable individuals and processes. Policies and processes should be identified and recorded, to ensure that records are protected from unauthorized addition, deletion and alteration.

Integrity refers to records being complete, and free from unauthorised alteration. Audit trails should be in place to demonstrate this. Integrity may also refer to the structural integrity of the physical and logical relationships amongst the content-related elements of a web site. If the structural of a website is impaired, its reliability and authenticity might be affected.

Usability means that records ought to be available and complete, so filing systems should be clear and unambiguous, and latest, authoritative versions of records should be easy to find and use. (US National Archives and Records Administration 2005)

2.3 A standard for Records Management

Almost all organizations must handle records, and there has been a good deal of material written on the topic. There is also an international standard, ISO 15489: Information and Documentation – Records Management (ISO/IEC 2001a; ISO/IEC 2001b), which provides advice on records management and the creation of as framework for a records management workflow. This is the first of several international standards we shall be discussing in the book, and, like the others, it has a dual significance for the organizations which use it. Firstly, it describes best practice. Secondly, adherence to the standards, which in the case of some standards can be certified by appropriate authorities, is a badge of good practice which the world at large can understand.

ISO 15489 is in two parts, the first constituting a general briefing, for all staff and management, on a framework for best practice in records management, and the second going into greater detail about designing and implementing a framework for records

systems. BSI Standards publish three books entitled ‘Effective records management’ which give practical advice on using the standard (Best 2002; McLeod 2002; Jones). 2003.

The standard sets out the characteristics of records and systems, which we’ve covered briefly, above, and principles for managing records – what records ought to be created, how to organise them and comply with legal policies, organizational needs and relevant standards. It also discusses the instruments required, such as a classification scheme and a controlled vocabulary, and how to document a retention schedule, describing what records ought to be kept, for how long and why, and recording the reasons for doing so.

Finally, it describes records management processes:

- ☐ Capture
- ☐ Registration
- ☐ Classification
- ☐ Access and security classification
- ☐ Identification of disposition status
- ☐ Storage
- ☐ Use and tracking
- ☐ Implementation of disposition

The standard has been adopted, or practices based on it have been adopted and recommended by the National Archive of Australia, the UK National Archive, the US National Archives and Records Administration (NARA), numerous UK county councils and universities worldwide. (Higgins, 2007)

3 The Information Commissioner’s Office

UK Information Commissioner's Office (ICO) is ‘The UK’s independent authority set up to **uphold information rights in the public interest,** [emphasis in original] promoting openness by public bodies and data privacy for individuals’ (Information Commissioner's Office 2012). As the quote suggests, the ICO has responsibility for providing advice on a range of legislation and regulation. In addition to those discussed in this chapter, it covers ‘The Privacy and Electronic Communications (EC Directive) Regulations 2003’, which cover such matters as nuisance telephone calls and ‘spam’ emails, and the INSPIRE regulations, which oblige UK public authorities to release information about spatial data sets. The ICO publicises the legislation, produces guides to compliance, maintains a register of data controllers, carries out audits, deals with complaints and monitors compliance. It has powers of enforcement – it can currently issue monetary penalties of up to £500,000 (Information Commissioner's Office 2013), can issue enforcement notices and bring criminal prosecutions. Its website [http://ico.gov.uk] is the definitive source of information and advice on these matters.

The reference to an ‘EC Directive’ in ‘The Privacy and Electronic Communications (EC Directive) Regulations 2003’ is because of the way that European Community legislation works. The EC issues Directives, which set out goals, to meet which, specified member communities, or all of them, are bound to implement laws, within a certain specified

period. How the law is implemented is at the discretion of the member state, because they may have different existing legislation, and so need different adjustments to bring that into line with EC Directives. Under the European Communities Act 1972, which is a piece of UK legislation, the UK parliament can implement, by means of Regulations, changes which require to be made to UK law. This gives a certain common purpose to the laws of EC member communities, which we shall also see expressed in the Environmental Information Regulations, described later in this chapter.

4 The Freedom of Information Act 2000

The UK Freedom of Information Act 2000 (FOIA) applies to 'public bodies' as defined in the Act, in 'the following broad categories;
Government departments, legislative bodies, and the armed forces
Local government
National Health Service
Maintained schools and further and higher education institutions
Police
Other public bodies (this includes a list of individually named non-departmental public bodies) '
(Information Commissioner's Office 2012)

The Secretary of State can add to the list bodies which appear to be 'providing functions of a public nature' (Information Commissioner's Office 2012) or acting for public authorities under contract. The Secretary can also remove organisations from the list, if they appear no longer to be acting in this way. The list also includes publicly-owned companies, companies wholly owned by the Crown, and companies owned by public authorities. Consequently, a very wide range of organisations are subject to the Act, which was introduced following a 1997 white paper stating the government's intention to promote openness and trust, and to reduce unnecessary secrecy. The Act covers any recorded information, and requests can be made by anybody – they do not have to be UK citizens or residents. The FOIA applies in England, Wales and Northern Ireland – Scotland has separate, though similar, legislation, the Freedom of Information (Scotland) Act 2002 (FOISA), and its own Information Commissioner.

4.1 Requirements of the FOI.

There are two types of requirement under the FOIA – one concerns the publication of information by public authorities. These are required to publish information – every public authority must have a publication scheme approved by the ICO, and the ICO makes available a model scheme (Information Commissioner's Office 2008) on which individual authorities' schemes must be based. Material to be published and made available under this scheme includes information about what the authority does, how they spend their budget, their decisions, policies and procedures, the services they offer, and lists and registers they hold which relate to their functions. They must also publish methods by which the information will be made available (for example, some types of information may have to be viewed by visiting a display), and charges applicable to obtaining the information (for example, the costs of photocopying or postage). As implied

by these examples, the information does not have to be published on a website, although many authorities will find that a website is the most convenient way of publishing much of it.

The second type of information is that which might be requested by a member of the public, organisations, such as the press, and indeed other public authorities (although the ICO observes that such information needs can normally be handled through other channels). This covers all information other than that covered by the publication scheme. What must actually be supplied is the information contained in documents. Note that emails are regarded as being documents, but only those stored in an organization's system, not those in personal email accounts of employees. You are not expected to supply information that exists only in the sense that someone knows it, nor are you expected to combine existing information to answer questions, although doing so if the work involved is not excessive would constitute good practice. You are not expected to disclose information which is still in preparation for publication. You do not have to disclose information held on behalf of another organization.

4.2 Freedom of Information requests

The mechanism for requesting the information is a Freedom of Information request, which to be valid must be in writing, include the requestor's real name and a contact address, and describe the information required. Not every request for information will be an FOI request, and not every request should be treated as such. However, requests identifying themselves as FOI requests and fulfilling the criteria for validity must be so treated. Requests which do not satisfy the criteria, or are not framed as FOI requests should still be dealt with where possible, as a matter of simple helpfulness, and many requests will not in any case relate to recorded information, or can be dealt with easily by reference to the publication scheme, discussed above.

If the request is for personal information, it should be dealt with under the terms of the Data Protection Act, as a Subject Access request, and if it is for environmental information, it falls under the Environmental Information Regulations. Both these cases will be covered later in this chapter.

4.2.1 Time for compliance

If the request does not fall into any of these categories, it should be dealt with under the FOI, meaning that within 20 working days from the day following receipt of the request, the organization must make a written response. If requests are ambiguous, or if it is unclear what information is being requested, the organisation must contact the requestor and seek clarification, and the time within which it must comply begins once the clarification has been received. Once the information is identified, the organization must confirm whether or not they have it, and must provide it, if they do. There are circumstances under which the organisation may refuse to provide some or all of existing information requested, but it would normally still be expected to confirm the existence of the information, or of further information, if all of the information has not been provided. There are, however, instances where the organisation my refuse to provide all or some of

existing information requested, or may decline to confirm or deny the existence of the information. For example, if a public authority was asked about plans to inspect an organization, to confirm or deny the existence of such plans would give the organization the chance to prepare for inspection, and so give it an unfair advantage. In this case the authority has grounds under section 30 of the Act neither to confirm nor deny the existence of such information. The relevant exemption must be cited in the refusal, unless to do so would in itself confirm or deny the existence of the information, and the decision to apply this exemption from disclosure must, as always, be taken in the public interest (Ministry of Justice 2012a).

4.2.1 Format of information supplied

The requestor can state in the request how they want the information to be supplied, but the ICO advises that in the absence of such specification, any reasonable format will suffice. Costs may be charged for printing, photocopying and postage in this respect.

4.2.2 When an organization may refuse an FOI request

A request may be refused on the grounds that providing the information would be too expensive in terms of monetary cost or the cost in staff time, if the request is 'vexatious' or if it repeats a previous request from the same requestor. 'Currently, the cost limit for complying with a request or a linked series of requests from the same person or group is set at£600 for central government, Parliament and the Armed Forces, and £450 for all other public authorities.' (Information Commissioner's Office 2013b) It may be that the information is already available, or that it is in preparation for publication. There are also exemptions based on the nature of the information requested, for example, if its disclosure could result in harm to a person or an organization's commercial interests might arise from its disclosure. There are exemptions for personal information covered by the Data Protection Act, and there are 'absolute' exemptions relating to defence, security and international relations, for example. In cases where exemptions are not absolute, the organization is required to decide whether disclosure would be harmful or against the public interest – that is whether the public interest would be done a greater disservice by not supplying the information than by supplying it.

4.3 Publication scheme

Essentially, what this does is to pre-emptively make information available- you can respond to enquirers that the information is on your web site, thus appearing to have anticipated their request, and reducing the time pressure of an FOI request; you are ensuring that the information they find is what you intend to be found, so that it is not assembled under time pressure from other sources and presented in a less carefully considered format; you have effectively 'answered the question already' – since there is already a 'public-facing' answer to the enquiry, there is no perceived need for the enquirer to persist in their enquiry. We have transparency, openness, accountability, and the US see it as opening up the democratic process to inspection. Saying that the information is available on your web site is an acceptable, and even quite helpful, response to an FOI request, and the question should really be, why would you not adopt this strategy? It should serve to forestall the vexatious or time-wasting enquirer. Should

an enquirer persist beyond the published information, however, there is a definite need for a robust and defensible records management policy.

5 Data Protection

As stated in the previous section, one of the rounds on which a public sector organization may refuse to disclose information is that it is personal information covered by the Data Protection Act, so the next step in examining an organization's obligations is to look at what that means.

The Data Protection Act 1998 (DPA) is more widely applicable than the FOIA. Whereas the FOIA applies only to the public sector, the DPA applies to anyone handling personal data about individuals.

5.1 Data subject to the DPA

5.1.1 Data

The Act's definition of 'personal data' is quite complex. 'Data' is considered to be

- information which is being processed by computer, or is recorded so that it can be so processed.
- Information that is part of a 'relevant filing system', or is recorded so that it can be part of one.
- Part of an 'accessible record', which does not come into these categories but falls under section 68 of the Act, or
- Does not fall into any of those categories, but is recorded information held by a public authority.

These definitions cover computing systems and their storage media, filing systems from which information concerning an individual can be easily retrieved, and data which have been prepared for input to either of these types of system (for example, recorded on data input sheets, prior to actual input). The reference to section 68 concerns rights of access that existed prior to the DPA, to data that were not held on systems like computers and the 'relevant filing systems' referred to above. In order to preserve those rights, after the introduction of the DPA, they are listed in section 68 of the Act, and refer to individuals' heath records, individuals' educational records and "accessible" records held by local authorities concerning housing or social services.

5.1.2 Personal data

The next step in the definition brings us to 'personal data'. These are considered to be **'**data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.'

(Information Commissioner's Office 2013c)

The ICO notes that there are two important points about this definition. First, if the data held can be put together with other data, for example a key file identifying the anonymised interviewees of a research report, and used to identify individuals, then the interviews are personal data. The other is that opinions of, and declarations of intentions towards, individuals are personal data about those individuals. Examples here might be an email between managers expressing an opinion of an employee, or declaring an intention to influence the outcome of someone's interview for a post.

5.1.3 Sensitive personal data

Finally, 'sensitive personal data' are personal data relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Membership of a trade union
- Physical or mental condition
- Sex life
- Status as an offender or alleged offender
- Involvement in proceedings for an offence or alleged offence

There is a clear inference to be made from this list that the 'sensitivity' of the data results from the possibility of its being used to discriminate about the individual, and since it is data concerning facts which might not otherwise be obvious to those who do not have access to the data, it receives special treatment under the Act.

5.2 Requirements of the DPA

The DPA sets out requirements for the processing of personal data, and more stringent requirements for the processing of sensitive personal data.

'**Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

a) organisation, adaptation or alteration of the information or data,

b) retrieval, consultation or use of the information or data,

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

d) alignment, combination, blocking, erasure or destruction of the information or data.' (Information Commissioner's Office 2013c)

5.3 Data subjects, controllers and processors

More definitions now. The simplest is **data subject** – the person that the personal data is about. A **data controller** is a person or organization who has responsibility for the data – who decides the reason for which the data is being processed, and the manner in which it is processed. A **data processor** is a person or organization who, or which, processes data on behalf of a data controller. This might be as a result of an outsourcing agreement, for example where a call centre acts on behalf of another organization, using data about that organization's customers. The responsibility for processing the data in compliance with the Act still rests with the data controller, though. Every data controller, unless they are exempt, must register with the ICO. Exemptions are available to not-for-profit organisations, those who use personal data for very restricted purposes and with the agreement of the data subjects, personal address lists held by individuals, and the ICO publishes a self-test (Information Commissioner's Office 2013e)

5.4 Data Protection principles

These are the eight principles listed in Schedule 1 of the DPA:

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.

(Data Protection Act 1998)

4.5 The first principle – Conditions

As is often the case with legal documents, the language in the DPA is expressed so as to reduce ambiguity, rather than to make for easy reading. Although the principles are not in themselves particularly convoluted, they are followed in the Act by a section on their interpretation which is less easy to understand. The ICO also offers its own interpretation, and makes the point that in Principle 1, since the conditions which must be met in order for data to be processed are in addition to the requirement that the purpose for which it is being processed is 'fair and lawful', it is advisable to consider fairness and legality first. Just because the conditions are met, in other words, that does not ensure the fairness and lawfulness of what is being done.

The conditions themselves are in two sets, one of which relates to personal data, followed by a more restrictive set which relates to sensitive personal data – Schedules 2 and 3, respectively. In each case, at least one of the conditions in the applicable Schedule must be met.

5.5.1 Schedule 2 conditions

The first, and less restrictive, set of conditions are that the data subject, the person the data is about, has given his or her consent that the data be processed, or that the processing is 'necessary' for one of a number of reasons.

These could be for the performance of a contract to which the data subject is a party, or in order that a contract may be entered into.

There may be a legal obligation other than a contract on the data processor.

There may be a need to protect the data subject's 'vital interests' – quite literally – according to the ICO, this applies only to 'cases of life or death', for example, where disclosure of medical information could help in an accident victim's treatment.

Administration of justice, or the carrying out of 'statutory, governmental, or other public functions' is a condition which covers those bodies responsible for such functions, so that, for example, a police force or a government department, in the process of carrying out its functions, may process personal data without the data subject having given consent.

Finally, there is a 'legitimate interests' condition, which has three requirements. First, the processing must be necessary for the data controller's legitimate interests, or for those of a third party to whom they want to disclose the information. The ICO gives the example of a finance house disclosing the details of a defaulting customer to a debt-collecting agency (Information Commissioner's Office 2013d).

The second requirement, once the first requirement is met, is that the interests of the data controller and the data subject must both be considered. If the processing has unwarranted repercussions on the rights, freedoms or legitimate interests of the data subject, then the processing does not meet the requirement. The key word here is "unwarranted" – although in the debt collection example, the two parties might disagree about the action, the finance company has a reasonable right to try to recover its money.

Lastly, the data processing under this condition must be fair, lawful and in keeping with the provisions of the DPA.

5.5.2 Schedule 3 conditions

When processing sensitive personal data, in addition to at least one of the schedule 2 conditions being met, at least one of the schedule 3 conditions must be met.
These are, firstly, that the individual has given explicit consent, where 'explicit' would be taken to mean consent to processing those particular, sensitive, data, and not just the more general personal data already considered.

Secondly, where the processing has to take place so that the processor can comply with employment law.

Thirdly, where the data subject's 'vital interests' are at stake, but the data subject's consent has not been obtained, or cannot be obtained, or where another individual's vital interests are at stake, but 'the individual's consent has been unreasonably withheld.' This last one needs some untangling.

Fourth, that the data processing is done by a not-for-profit organisation, and does not involve disclosure of the data to a third party, unless with the individual's consent.

Fifth, that the individual has themselves made the information public. Here we might think of someone whose otherwise 'sensitive' information regarding their trade union membership or political affiliation is made known by them wearing badges, or publicly exhibiting political posters.

Sixth, if the processing is necessary in relation to legal proceedings.

Seventh, if the processing is necessary for "administering justice", and other public functions – essentially the same condition as the fifth condition in Schedule 2.

Eighth, if the processing is necessary for medical purposes, and is carried out either by a health professional or by somebody under the same duty of professional confidentiality.

Ninth, if it is necessary that the processing is done in order to monitor equality of opportunity, and with safeguards for individuals' rights. An example here might be if sensitive data about ethnic origin was collected by an employer.

"Necessary" in the last four conditions has quite a strict interpretation, meaning that there is no other reasonable way that the results referred to in each case could be achieved, and necessity cannot be simply due to the way the data processor chooses to operate.

5.5.3 Extensions to the Schedule 3 conditions

There are two Statutory Instruments which extend the scope of the Schedule 3 conditions:

Statutory Instrument 2000 No. 417: The Data Protection (Processing of Sensitive Personal Data) Order 2000
and Statutory Instrument 2002 No. 2905: The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002

These additionally provide for the processing of sensitive personal data, by, on behalf of, or for disclosure to, an 'elected representative' (a Member of Parliament, of National Assemblies, or of a local authority):

- in order to prevent or detect any unlawful act
- in order to protect the public against dishonesty or malpractice
- to be published in the public interest
- in order to provide confidential counselling, advice or any other service
- for carrying out of insurance business
- for monitoring equal opportunity regarding beliefs or mental health
- by registered political parties for legitimate political activities
- when it is necessary for research purposes
- when the processing 'is necessary for the exercise of any functions conferred on a constable by any rule of law.'

(The Data Protection (Processing of Sensitive Personal Data) Order 2000)

Remember that all this is just in order to comply with the first of the eight principles. The data has to be processed fairly and lawfully, and at least one of the appropriate set of conditions has to be met. The ICO points out that overall fairness should be a more important consideration than obtaining consent, which, although listed first in each schedule, is, in each schedule, only one of many equally valid conditions.

5.6 The second principle

Now that we have established whether processing can take place at all, the second principle begins to examine how the processing must be done, and begins with the reason for which the data is obtained. 'Obtaining' may not appear to be 'processing', but remember that 'processing' encompasses many operations relating to the data. The second principle says that the data must only be obtained for 'specified and lawful purposes', and that it must not be 'further processed' in a manner 'incompatible' with those purposes. In other words, before you collect personal data, you must have a justification for doing so, and that purpose is the only thing you are allowed to use the data for – if you want to use it for something else as well, that requires separate justification, perhaps a different agreement with the data subject and perhaps a separate notification to the ICO.

As an example, suppose an organization collects employees' personal data for Human Resources (HR) and payroll purposes, and is registered with the ICO as a data controller in those respects. If a member of the public telephones, asking for contact details of that employee, who is an old friend of theirs, the organization should not disclose the information, because that is not the purpose for which the data were collected. Disclosure is 'processing', and although the employee will have given consent to supply the data, and keeping the data for HR and payroll is necessary for the organization's legitimate interests, it is unlikely that the employee has consented to allow their personal data to be disclosed to all.

Another example occurs quite frequently in universities – after assessments, there is a phone call from a student's parent, or someone purporting to be a student's parent, asking for their mark in the assessment. Disclosure to this person is not the reason why records of student marks are kept, and apart from the question of identity (a telephone call would not be sufficient to identify even the student themselves), the marks should not be disclosed.

4.7 The third, fourth and fifth principles

These can be considered as a group – as the ICO notes (Information Commissioner's Office 2012b), they are all related to data standards, a topic to which we shall be returning in Chapter 5, but which is probably easier to grasp in this scenario of very well-defined, and relatively simple, data.

The principles stipulate, respectively, that personal data should be

- adequate, relevant and not excessive in relation to the purposes for which they are processed

- accurate and, where necessary, kept up-to-date, and
- kept for no longer than is necessary for the purpose, or purposes, for which it has been processed

(Data Protection Act 1998)

The standards are inter-related because relevance and accuracy are closely connected, as are being kept up-to-date and for no longer than is necessary, which could also be considered excessive, and so on. The Act splits the requirements down like this for clarity of definition, but, in practice, the data controller will want to consider them together, or at least be always conscious of the linkages amongst them.

5.7.1 The third principle

The third principle is about the amount of data that is held – enough to serve the purpose for which it is processed, but no more than that, remembering that 'processing' includes storage. For example, a conscientious firm who install replacement windows might build up a bank of information about the properties and owners of houses in an area, and approach them with a view to selling them new windows. This might be done by telephoning the properties, and asking about ownership/tenancy, number of rooms, number of windows, and so on. It would be appropriate for the organisation to retain more detailed information about the owners and properties where interest is expressed in the product, but only sufficient information about the others to ensure that they are not approached again.

A social club planning a group holiday would probably collect next-of-kin contact details for those going on the holiday, but it could be considered irrelevant and excessive to do so for all members – information should not be kept just in case it might be useful in future.

5.7.2 The fourth principle

Accuracy and currency of information appear quite simple, but some questions of interpretation can arise. Not all information can be checked, but the data controller should take reasonable steps to do so, and ensure that the source of personal data is known and recorded. If the accuracy of data is challenged, the challenge and the need to update the data should be considered. At a fairly mundane level, and far pre-dating the DPA, this is one of the reasons why the minutes of meetings are read and approved by the next in a series of meetings, so that an accurate record of the proceedings is kept. There may be cases where personal data should be kept about something which is not true, in a sense. For example, if disciplinary proceedings are taken against an employee, who is found not to have breached the relevant regulations, then the employee should not be recorded as having breached the regulations, which seems quite obvious. However, if the employee requests that reference to the proceedings be removed from the records, there are good reasons for refusing to do so, because that record is accurate.

The social club from a previous example may hold records of names and addresses of lapsed members for accounting or archival purposes, but is not obliged to update these records with subsequent changes of address, although this would be the case with current

members. If information is held for certain purposes, such as historical research, then the fact of updating it might invalidate those purposes. The information should be accurate with respect to the period it reflects, and this should be recorded.

5.7.3 The fifth principle

Just as these three principles, three, four and five, can be seen as an introduction to data quality, principle five in itself introduces the idea of the **record retention schedule**, a central component in the Records Management toolkit. The principle itself is stated simply: “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.” (Data Protection Act 1998) However, as the ICO points out, in practice this implies reviewing why you keep the personal data, how long you need to keep it for, and ensuring that it is disposed of securely when it is no longer needed. The ICO adds that information which is out-of-date should be updated, archived or securely deleted. This last requirement is not immediately obvious from the statement of the fifth principle alone, but is implicit in reading it in conjunction with principles three and four – if you keep the data, it must be accurate. If it is to be accurate, that means it must be updated when necessary. If it is being kept for historical purposes, it must be archived, so that it is no longer regarded as current. If none of these apply, it is no longer necessary, so must be deleted, and this must be done securely, so that there is no danger of its being mistaken for current data, or otherwise misused. Since an organization may be keeping many types of information, for many purposes, it will probably be desirable to formalize the procedures involved in dealing with information into a records retention schedule. All records should be reviewed regularly for accuracy and currency, but for certain classes (or **series**, to use the Records Management term) of records, decisions can be made in advance, as a matter of policy, which decide their eventual disposal, whether to archive or secure deletion, and the timing of this disposal. Often, this will be a matter of organizational policy (for example, an organization might store customer sales transaction records for three years, in case of returns or guarantee claims) or of legal or professional requirement (the educational records of a midwife might be retained for as long as she continues in practice). The reason for the decision should be recorded in the schedule, alongside the record series and the decision itself. In many cases, where records are stored electronically, the process can be semi-automated (subject to human confirmation and override, in the event of anomalies).

5.8 The sixth principle

The sixth principle is that data shall be processed in accordance with the rights of individuals under the act, and there are six of these. An individual has:

- a right of access to their personal data
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

(Information Commissioner's Office 2013f)

The first of these rights is expressed through a **Subject Access Request** (SAR), the individual's mechanism under the Act for finding out what personal data regarding them is being processed. The SAR is a very important topic in practice, and will be discussed following this discussion of the principles. The others are rights to modification of either the data or the processing, and are explained in detail by the ICO (Information Commissioner's Office 2013f).

5.9 The seventh principle

The seventh principle is 'Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' (Data Protection Act 1998) Chapters 4 and 5 of this book will deal with security measures regarding this, and other, information.

5.10 The eighth principle

The final principle concerns the sending of data outside the European Economic Area (EEA), and can be summarized as stipulating that personal data must not be sent outside the EEA, unless to a jurisdiction (country or territory) which provides at least the same level of rights and freedoms to individuals regarding their personal data as they have within the EEA. Remember from the previous discussion that the structure of EC directives and local implementations guarantees that all EC member countries will have legislation with equivalent impact, although this situation may have been reached by different routes in different countries. The EEA countries are the27 EU member countries, plus Norway, Lichtenstein and Iceland, and the EC maintains and publishes a list of other, or 'third countries', which it recognises as 'providing adequate protection' (European Commission 2013)

The list includes the 'Safe Harbor' scheme, under which US companies may voluntarily sign up to abide by seven principles of data processing, and render themselves accountable to the Federal Trade Commission or other oversight schemes for doing so. The scheme is explained on the US Department of Commerce web site (Export.gov 2012).

The final entry on the list is 'the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection'. This concerns a 2007 agreement that the US authority would regulate and adequately protect such data, supplied by EU airlines. The data is required by the US authorities for security purposes, but, because the US is not a 'third country', and the US Department of Homeland Security is not part of the 'Safe Harbor' scheme, a separate agreement was reached.

5.11 Subject Access Request

A Subject Access Request (SAR) is the means by which an individual can find out what data regarding them is held by an organisation. Note that some information requests which may initially appear to be simple enquiries, or which may appear to fall under the

Freedom of Information Act or the Environmental Information Regulations, will in fact relate to personal data, and thus come within the remit of the DPA. If the data requested is personal data relating to the individual, this should be treated as a SAR, but if, as is more likely, the personal date relates to others, the provisions of the DPA regarding disclosure would apply. You must respond to a valid SAR within 40 calendar days, telling the individual what information about them you hold, ands providing them with a copy of the information.

5.11.1 Validity

A valid SAR must be made in writing, although email and fax count as equivalent. It would, however, be good practice to treat a verbal request as if it were valid, or at least to explain how to make a valid request. It is also reasonable to make the necessary adjustments to enable people with disabilities to make valid requests, where they might otherwise be disadvantaged in doing so, as well as providing the information in an appropriate format to allow them to use it (for example, Braille, large print, or a computer file which could be used in a text-to-speech application).

5.11.2 What you must provide

As a data controller, you must provide the information you hold about an individual, but not necessarily the documents containing that information. This should be the information you hold at the time you receive the request, although if at that time the information is under routine amendment, or is due for deletion, it is reasonable to provide the information you hold at the time at which you respond to the request. However, you may not amend or delete the information if this would not have been routine, and if your organization is subject to the FOIA, that would constitute an offence.

The information must be in an ‘intelligible form’, which means that an average person should be able to understand it. Codes, for example, should be explained, but handwriting would not have to be transcribed, nor would translation into another language be expected.

5.11.2 Time for compliance

In most cases, you have 40 calendar days to respond to a request, starting with the day following the day you receive the request. In some cases, you may have to ask for a clarification of the request, in which case the time does not begin until you receive the clarification, but you should not use this as a mechanism for extending the time you take to respond. The same provision applies with respect to fees.

5.11.4 Fees

An organization may charge a fee (currently £10 maximum) for providing information, although organizations holding health or education records may, under certain circumstances, charge up to £50. If a fee is payable, but has not been sent with the

request, you should contact the requestor and inform them of the need for payment. The 40 day period for responding to the request does not begin until the payment is received.

5.11.5 Information about other people

Individuals may ask a third party, such as a friend or a solicitor, to make a SAR on their behalf, or it may be that someone with the authority to manage an adult's property or affairs makes such a request on their behalf. You need to be satisfied that the third party is entitled to such authority, although it is their responsibility to provide the evidence to substantiate their claim. It may be that you decide that the nature of the information is such that it is more appropriate that it be sent directly to the individual, who can then make the decision as to whether to share it with the third party.

5.11.6 Information about children

Personal data about a child belongs to them, and it is they who have the right of access to it, although in the case of very young children, this right may be exercised by a parent of guardian. It is your responsibility to decide whether a child is mature enough to understand their rights, to understand what it means to make a request, and to interpret the resulting information. If so, the response should be to the child, rather than to anyone else. In cases where this is a difficult decision, the ICO recommends that you also consider:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

(Information Commissioner's Office 2013g)

In Scotland, it is presumed in law that a child of the age of 12 or more is capable of making a SAR. Although this does not apply elsewhere in the UK, it would appear to set a reasonable guideline. The ICO also notes that capacity to make the request does not imply capacity to understand the implications of sharing the information, or to consent to doing so.

Obviously these are potentially very difficult decisions for the data controller to make, since so much is open to interpretation. It might be advisable to seek legal advice under these circumstances, or even to arrange an advisory visit from the ICO, in order to

prepare for such an eventuality, if your organization routinely processes such information. (Information Commissioner’s Office 2013h)

5.11.7 Information about others

It may be the case that in order to provide information about an individual, you would also have to provide personal information about other people. If the other parties give their permission, this is not a problem, but if their permission cannot be obtained, you must decide whether it is reasonable to provide the information without their consent. The Act states that you do not have to comply with the request unless the third party has given permission, or it is reasonable to comply without such permission. Again, this is a matter or weighing the rights of the person making the request against the rights of the third party, and you will need to take all the relevant circumstances into account.

5.11.8 Disproportionate effort

It may be that the effort involved in supplying a copy of the information held necessitates effort that is disproportionate to the benefits to the individual, in which case you do not have to supply a copy of the information in permanent form. This could be because of the volume of information, for example, or because of the way in which it is held. For example, an individual’s transactions with a shop of which they are a customer might be recoverable in detail for only the most recent accounting period, whereas recovering details of older transactions might take considerable effort. However, the waiver only applies to supplying the information in permanent from, not to the work involved in locating it. Because the right to information is so important, it would be very unusual for this to be a valid reason, and it would probably be possible to provide the information in some alternative manner.

5.11.9 Repeated or unreasonable requests

You do not have to answer the same, or a very similar, request, unless a reasonable time has elapsed since the last time the request was made. This might depend on how sensitive the data is, why it is being processed or how frequently the data changes. However, there is no limit on the number of requests an individual can make to an organization.

6 Environmental Information Regulations

The Environmental Information Regulations implement EC directive 2003/4/CE, itself a result of the Aarhus Convention, 1998, which was signed by the EU and the UK. They apply to 'public authorities' - local authorities, government departments, police, universities, the NHS and some bodies that do public works that affect the environment.

There is a presumption in favour of disclosure - you disclose information unless there is a good reason not to.
You have obligations a) actively to make the info available, by electronic means if possible, and b) to respond to requests, which could be from anyone.

There is a code of practice for fulfilling your Obligations under EIR, (Code of Practice – Environmental Information Regulations 2004 2005) and a code of practice (code 46) covering the responsibilities of public authorities under FOI and EIR (Ministry of Justice 2012b). Whereas under the FOIA you have a duty to maintain and publish a publication scheme, this does not apply under EIR, although it would appear to be a practice which would be consistent with the first obligation, and a way of demonstrating good practice.

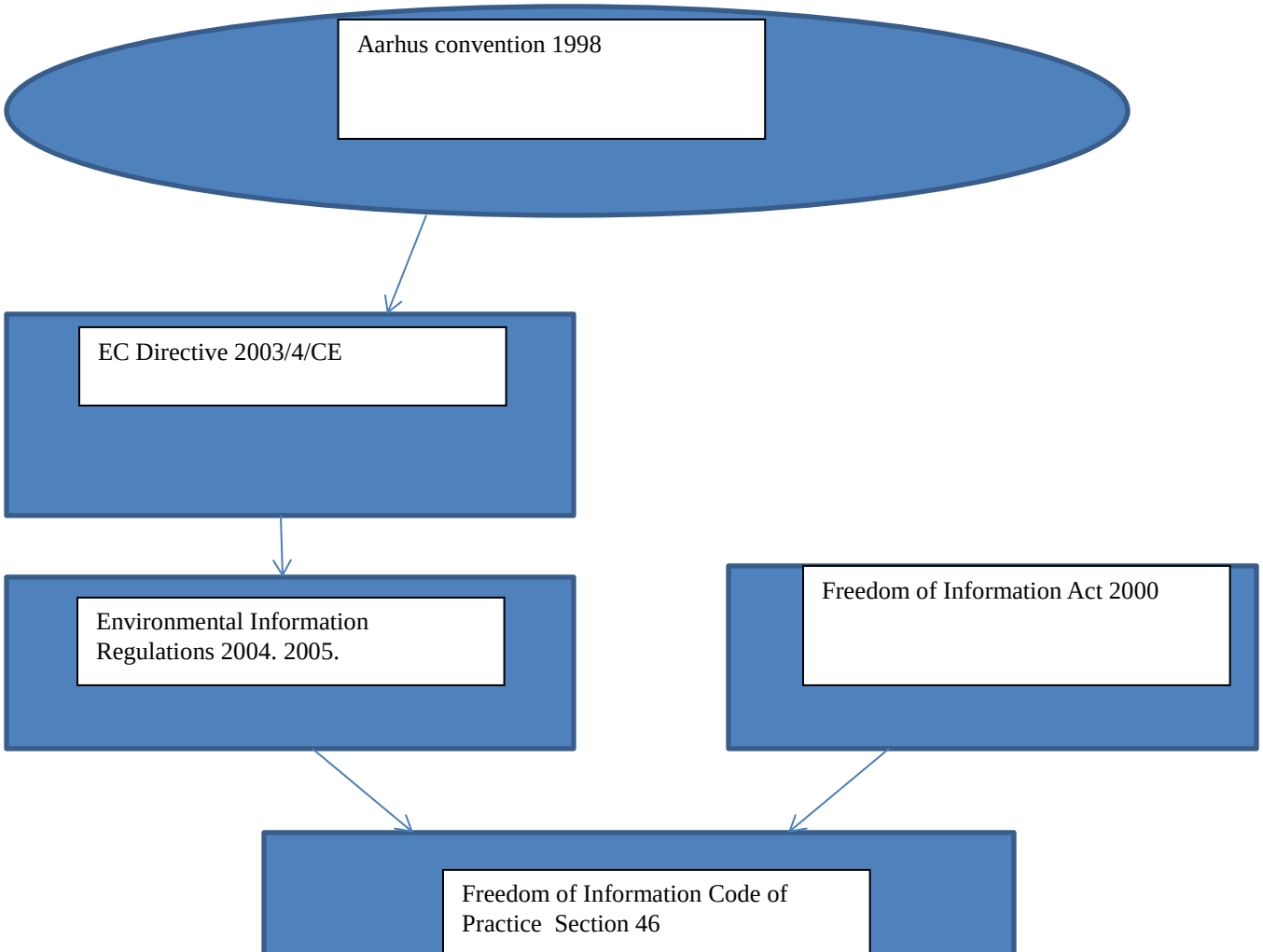

Figure 2 The code of practice gives guidance on records management according to the Regulations and the Act

According to the ICO:

> The minimum information you must routinely publish is listed in Article 7(2) of the European Directive 2003/4/EC. This includes policies, plans and procedures relating to the environment, reports on the state of the environment, environmental impact studies and data taken from monitoring activities and risk assessments that affect or are likely to affect the environment. This may cover public registers of environmental information you maintain under another piece of legislation, your organisation's carbon emissions data, or details about external renovation and building work. You must also publish facts and analyses of facts that are relevant and important to major environmental policy proposals.

6.2 Copyright, database and Intellectual Property Rights (IPR)

Disclosing information under EIR should not have any effect on these rights. You are not allowed to require people to sign a statement that they will not infringe copyright, although you may include a copyright notice with the information you do disclose, and you can make a claim in the courts regarding breaches of copyright. These rights considerations should not be a bar to disclosure, but there is an exemption to the disclosure requirement, where disclosure could adversely affect IPR.

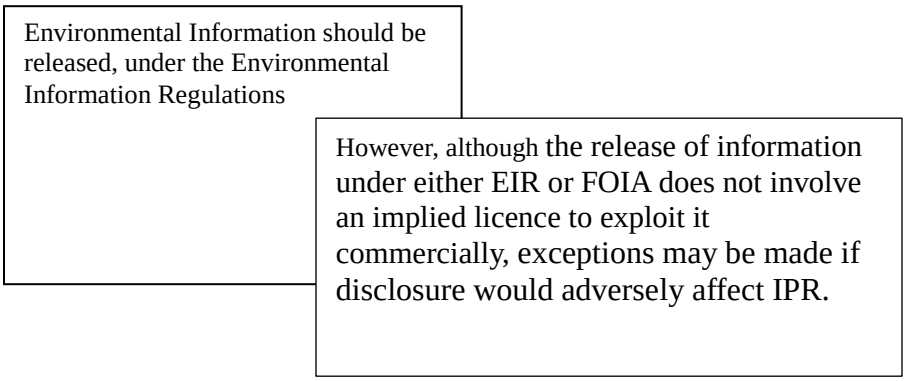

Figure 3. Environmental Information Regulations and IPR

6.3 Property searches

Local Authorities (England) Charges for Property Searches Regulations (CPSR) is another potential area of overlap, since many property searches will be of an environmental nature, and the charging policies for each are different. The CPSR does not apply where the local authority a) can charge for access to property records or b) has to supply records free of charge under another enactment. If the information is environmental, EIR provided discretion for making a reasonable charge, and define when the authority cannot charge.

6.4 What you must provide

6.4.1 Time for compliance

The information must be provided within 20 working days, beginning the day following the day that the organization receives the request, or the day following receipt of clarification of the original request, should this be required. It is good policy to refer to the time limit in the initial response to, or acknowledgement of, the request. If a request is particularly complex, an extension of up to an additional 20 days can be claimed, but in this case, the requestor should be told.

6.4.2 Fees

If a fee is to be charged, and advance payment is required, the 20 day period does not begin until the fee is received, which must be within 60 days of the original request.

7 Policy

In each chapter, we'll be discussing the contribution that it can make towards a comprehensive Information Governance and Assurance policy for your organization. The main points arising from this chapter are the importance of good records management in responding to information requests, and the fact that much of the work involved can be carried out in advance, by publishing information actively.

7.1The Records Retention Schedule

It ought to be clear that compliance with the various regulations is desirable for a number of reasons. First, there are the ideals of openness and accountability which influenced the framing of the regulations in the first place. Secondly, providing the information is providing a public service, as is protecting it from misuse. Thirdly, the ability to produce information on any relevant topic, at short notice and without compromising the normal operations of your organization, is a sign of a well-organized and efficient approach to information management. Finally, avoidance of the quite considerable sanctions at the disposal of the ICO and its counterparts in other jurisdictions ought not to be the prime incentive towards compliance, but can certainly act as a spur.

It should be remembered that having a retention schedule is important for many reasons – the most obvious being that unneeded records aren't kept for longer than necessary, with the resultant waste of storage space, and perhaps increased difficulty in retrieving the records which **are** needed. Record retention requirements are not intended to hinder the carrying out of business, and it is not feasible to keep everything.

The retention schedule should list the different series of records, the person or department having 'ownership' of the records, the point at which they become 'inactive', and the method of their disposal – archiving or destruction. Each entry should also list the justification for this decision, which will usually be either a piece of legislation, advice from a body such as the Joint Information Systems Committee (JISC) or the ICO, or organizational policy. When a record reaches the end of its useful life, the disposal routine should be triggered. In electronic records systems, this can often be done semi-automatically – there should always be a human verification of the disposal. Retention times may vary widely – a student midwife's training records may be preserved for her whole working life, whereas the personal data of a survey subject should normally be disposed of on the termination of the survey.

In common with many public authorities, the ICO publishes its own Records Management policy (Ebitt 2009), and it also discusses the benefits of a disposal schedule (Information Commissioner's Office 2013i)

7.2 The publication scheme

Publication is required by the FOIA, and is not required, but is certainly advisable, under the EIR. You can save your requestors' time and effort, and yourself time, effort and stress, by actively publishing, probably via a web site, as much of the information as you can that would not be subject to an exemption. Obviously, this does not apply to personal information, where the emphasis is on accuracy and secure processing and disposal, but the same effort should be put into checking, organising and making retrievable personal information as if it were to be published, because it is, but to a very restricted audience, typically of one.

8 The role of the information professional

There is a great deal of complexity discussed in this chapter, and there are many further ramifications to each piece of legislation which need to be considered. As an information professional, your role is quite likely to involve handling requests, or enquiries which might resolve to requests, in an efficient and effective manner. It would be a good idea to try to ensure that information requests, whether formal or not, are channelled through one authoritative point, which may well be your role. Other 'outward facing' staff should be encouraged to channel requests in your direction, and it is quite easy to 'sell' this idea – they are helping the enquirer, but not taking on any additional work themselves. The data protection principles should certainly form part of staff induction or training in any public authority or other data controller.

Keeping abreast of the legislation is obviously important, and it is an area which is subject to fairly frequent updates.

Remember that the publication scheme is not an imposition, but a very useful tool – you do not want to spend all your working life 'firefighting'.

Finally, note that many of the enquiries you might receive can be dealt with informally, without ever reaching the status of a full-blown information request – this is good practice, and makes the whole process of access to information run much more smoothly for everyone involved.

Discussion points

1. You work in the Planning Department of a local authority, and receive a request for any information you hold regarding planning applications by a particular individual for a property at a particular address. What would your response be?
2. What measures might you take to ensure the security of personal data held by your organization?
3. You work in a hospital, and are asked by the mother of a14 year old patient for details about his treatment. How should you respond?
4. As the curator of a military museum, you are asked for details of the service of a named individual, who may have served in your regiment at indeterminate dates. How should you respond?
5. The university in which you are the Records Manager receives an enquiry about accidents related to harmful chemicals in the last 5 years. What do you do?

References

Best, D., 2002. *Effective records management. A management guide to the value of ISO 15489-1*, London: BSI

Code of Practice – Environmental Information Regulations 2004. 2005. [online] Available from:

http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Environmental_info_reg/Detailed_specialist_guides/ENVIRONMENTAL_INFORMATION_REGULATIONS_CODE_OF_PRACTICE.ashx (Accessed (17/06/13)

Data Protection Act. 1998. [online] Available from: http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 31/05/13)

Ebitt, S., 2009. *Records Management policy.* [online] Information Commissioner's Office Available from: http://www.ico.org.uk/~/media/documents/library/Corporate/Notices/RECORDS_MANAGEMENT_POLICY.ashx (Accessed 19/06/13)

European Commission. 2013. *Commission decisions on the adequacy of the protection of personal data in third countries.* [online] Available from: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (Accessed 09/06/13)

Export.gov. 2012. *Main Safe Harbor homepage.* [online] Available from: http://export.gov/safeharbor/ (Accessed 09/06/13)

Freedominfo.org. 2013 *Rwanda publishes new law on right to information.* [online] Available from: http://www.freedominfo.org/2013/03/rwanda-publishes-new-law-on-right-to-information/ (Accessed 19/06/13)

Higgins, S., 2007. *ISO 15489*. [online] Edinburgh: Digital Curation Centre. Available at http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/iso-15489 accessed (11/11/13).

Information Commissioner's Office, 2008. *Model publication scheme.* [online] Available from: http://www.ico.org.uk/for_organisations/freedom_of_information/guide/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/generic_scheme_v1.ashx (Accessed 30/05/13)

Information Commissioner's Office, 2012. *Public authorities under the Freedom of Information Act* [online] Available from: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/public_authorities_under_the_foia.ashx (Accessed 28/05/13)

Information Commissioner's Office, 2012b. *Introduction to Principles 3, 4 and 5 of the Data Protection Act* [online] Available from: http://www.ico.org.uk/for_organisations/data_protection/the_guide/information_standards/introduction (Accessed 08/06/13)

Information Commissioner's Office, 2013. *Enforcement.* [online] Available from: http://www.ico.org.uk/enforcement (Accessed 30/05/13)

Information Commissioner's Office, 2013b. *When can we refuse a request for information?.* [online] Available from: http://www.ico.org.uk/for_organisations/freedom_of_information/guide/refusing_a_request (Accessed 30/05/13)

Information Commissioner's Office, 2013c. *Key definitions of the Data Protection Act.* [online] Available from: http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

Information Commissioner's Office, 2013d. *The conditions for processing.* [online] Available from: http://www.ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing (Accessed 07/06/13)

Information Commissioner's Office, 2013e. *Register (notify) under the Data Protection Act* [online] Available from: **http://www.ico.org.uk/for_organisations/data_protection/registration** (Accessed 08/06/13)

Information Commissioner's Office, 2013f. *Principle 6 of the Data Protection Act - Guide to Data Protection.* [online] Available from: http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_6 (Accessed 09/06/13)

Information Commissioner's Office, 2013g. *Access to personal data.* [online] Available from: http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_6/access_to_personal_data (Accessed 16/06/13)

Information Commissioner's Office, 2013h. *Advisory visits.* [online] Available from: http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/advisory_visits (Accessed 16/06/13)

Information Commissioner's Office, 2013i. *Retention and destruction of requested information.* [online] Available from: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Practical_application/retention-and-destruction-of-requested-information.ashx (Accessed 19/06/13)

ISO/IEC. 2001a. *ISO 15489-1: 2001 Information and documentation -- Records management -- Part 1: General* Geneva: ISO/IEC.

ISO/IEC. 2001b. *ISO 15489-2: 2001 Information and documentation -- Records*

management -- Part 2: Guidelines. Geneva: ISO/IEC.

Jones, P., 2003. *Effective records management: Performance management for BS ISO 15489-1*, London: BSI

Kuner, C., 2010. *Data protection law and international jurisdiction on the internet (part 1).* International Journal of Law and Information Technology vol. 18 no. 2. Oxford University Press. pp 176 – 193. Available from: http://ijlit.oxfordjournals.org/content/18/2/176.full.pdf+html (Accessed 19/06/13)

McLeod, J., 2002. *Effective records management. Practical implementation of ISO 15489-1*, London: BSI

Ministry of Justice. 2012a. *Neither confirm nor deny.* [online] Available from: http://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/exemptions-guidance/foi-exemptions-ncnd (Accessed 17/06/13)

Ministry of Justice. 2012b. *Freedom of Information Code of Practice.* [online] Available from: http://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/code-of-practice (Accessed 17/06/13)

Penn, I. A., Pennix, G. B. and Coulson, J., 1994. *Records management handbook.* Cambridge : Cambridge University Press

The Data Protection (Processing of Sensitive Personal Data) Order 2000 [online] Available from: http://www.legislation.gov.uk/uksi/2000/417/schedule/made (Accessed 08/06/13)

US National Archives and Records Administration. 2005. *NARA guidance on managing and maintaining web records.* [online] Available at: http://www.archives.gov/records-mgmt/policy/managing-web-records.html (accessed 12/11/13)