Web Links
Links to websites are highlighted in the text and, when using the Guidelines online, can be clicked through directly. If using a printed out version of the text you will find the full web addresses set out section by section in Appendix 4.

Chartered Institute of Library & Information Professionals (CILIP)
December 2009
Revised May 2011
Registered Charity Number: 313014

For inquiries about the Guidelines contact:
Policy & Advocacy Unit, CILIP,
7 Ridgmount Street, London, WC1E 7AE
Email: policy@cilip.org.uk
1 Introduction

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

“21st century themes for regulating the privacy and integrity of personal information involve greater emphasis on trust, confidence, and transparency. Safeguarding personal information has become a major reputational issue for businesses and governments.”

---

1 Article 8 of European Convention of Human Rights, in Sch. 1 Human Rights Act 1998

ii Information Commissioner’s Office press release (2009)
[Accessed 29th September 2009]
There is increasing anxiety in information work about the tension between the freedom of access to information and the right of an individual to privacy concerning personal data. Recent legislation has not clarified that tension. As part of CILIP's advice to members these guidelines have been produced to support individual members in adhering to the CILIP Ethical Principles and Code of Professional Practice and to protect the interest of the users of their service. CILIP members can seek confidential advice from the Ethics Panel (ethics@cilip.org.uk).

A task and finish group (see Appendix two) was set up by CILIP's Policy Forum to:

- Create principles about privacy, and members’ responsibilities for protecting data and people’s freedoms (including the need to differentiate between individuals leading or working in a service and the context in which they work)
- Develop statements or policies to reflect these principles with regard to handling requests for information, the use of standard forms/procedures and examples of good practice.

Many organisations will have policies and practices in place but it is important that we all understand the landscape in which we are working. The guidelines are part of the responsibility of the Ethics Panel and will develop as legislation changes.

Information professionals collect data from their users in order to provide the most efficient and effective service. We must protect the personal data we collect and be very clear to our users why we collect the data, how we store it, how we process it and for how long we keep the data. Occasionally by law we may be required to give personal data to a third party; we need to ensure that this is justified.

The impact of technology and the ease with which data is now generated, stored, processed and published means we must be even more vigilant about protecting the interests of the users. The range of stakeholders using any particular service is wide so the policies and practices we employ in that protection must be robust whilst still working within the law.

The guidelines are in six sections:

1. Introduction
2. Privacy
3. Keeping users informed
4. How to handle requests for data
5. The law and the privacy of users
6. CILIP's Ethics Panel

Sections two to four have a short discussion, general principles or codes of practice, further information and examples of good practice (these may be added to and updated). Section five is a brief guide to the legislation.

It is hoped that these guidelines will enable information professionals at all levels to understand the basic principles of user privacy and to reflect on their own practice and that of their employing organisation.

The balance between user privacy and the need to have access to information, as stated above, is not simple. Most information professionals are required to abide by the information policies of their employing organisation but that does not take away individual responsibility. We can seek to improve both policies and practice through normal channels. However, if there are areas of real concern then as information professionals we must bring those to the attention of senior managers or even to the chief executive of the organisation if there is no response from senior management. Beyond that members can share the concern with CILIP's Ethics Panel, and where necessary, get support to challenge practice.
Checklist of what you can do

Judgement has to be made as to what action is appropriate in each context. Few issues will go to the top levels of action but when concerns occur:

• Research the issue
• Raise concerns with appropriate colleagues
• Raise concerns with your line manager
• Raise concerns with your mentor
• Raise your concerns with CILIP’s Ethics Panel which will deal with any requests on a confidential basis. (You are strongly advised to do this before taking more serious steps such as reporting a concern outside your own organisation)
• Raise your concerns with senior management
• Raise your concerns with the governing body
• Instigate the employer’s own whistleblowing process where necessary. Many, although not all, employers have such a process. Under certain circumstances the Public Interest Disclosure Act 1998 affords some employment related protection to those making disclosures
• Report organisation to the Information Commissioner’s Office
• Go public – you should seek legal advice before doing this as you could lay yourself open to charges of defamation
2 Privacy

2.1 Personal data

What is personal data?

Personal data is data pertaining to an individual that may include name, address, contact details, work details, age, sex, data on loans, internet use and interlibrary loan requests. Library and information staff now have greater potential for collecting and storing many types of personal data and need to be vigilant in guarding public trust (Sturges et al 2003). We should be clear what personal data we collect, why we keep it and for how long. We also need to inform users of our policies and practice.

2.2 Personal data – the principles

“Library users should have the right to personal privacy and anonymity. Librarians and other library staff should not disclose the identity of users or the materials they use to a third party.”

(International Federation of Library Associations and Institutions Statement on libraries and intellectual freedom)

One of CILIP’s Ethical Principles states we should have:

“Respect for confidentiality and privacy in dealing with information users” and the associated Code of Professional Conduct cautions all practitioners to “protect the confidentiality of all matters relating to information users, including their enquiries, any services to be provided, and any aspects of the users’ personal circumstances or business.”

---


IFLA (1999) Statement on libraries and intellectual freedom

CILIP Ethical Principles for library and information professionals
The key message from the American Libraries Association (ALA) is:

“privacy is essential to the exercise of free speech, free thought and free association... librarians have a responsibility to protect the privacy of patrons while responding to legitimate national security concerns.”

(ALA Privacy Tool Kit)

The (UK) Data Protection Act 1998 also sets out eight legal principles governing the use of personal data:

• Personal data shall be processed fairly and lawfully
• 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
• Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
• Personal data shall be accurate and, where necessary, kept up to date
• Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
• Personal data shall be processed in accordance with the rights of data subjects under this Act
• 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
• 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

Checklist

These are some of the questions you may need to consider:

• Has there been an audit in your organisation of all records which link users’ personal data to enquirers, borrowing or other services?
• Does your organisation gather the minimum amount of personal data necessary for any library operation?
• How does your organisation ensure that personal data remains accurate?
• Is information or data connecting a user to a particular transaction retained for only as long as needed for normal operations?
• Is access to personal data restricted to a limited number of appropriate library personnel, plus, where appropriate, to agreed personnel in the host organisation?
• Does your organisation have a clear policy on data sharing?
• Does your organisation have a privacy policy that covers all kinds and types of records?
• Are these policies publicised effectively?
• Are users advised on how best to protect their privacy?
• Have staff been trained in privacy issues?
• Does your organisation scrutinise contracts and/or licences as to personal data which is collected by third parties e.g. providers of electronic information services? And do they raise the issue of personal data retention with contractors?

Privacy action points

The safest way not to compromise the privacy of individuals is not to collect personal data in the first place. The last five action points below are ways of achieving this technically through the automatic deletion of
computer generated personal data. However, some library services may want to collect this information as it can provide a basis on which to enrich and personalise services offered by the library. It is important that decisions are formally made regarding these things with a full understanding of the implications.

- Avoid library practices and procedures which place user personal data on public view
- Display only the appropriate personal data on users for each procedure
- Find ways to separate user names from interlibrary loan records
- Make it clear on your website where users can opt in or opt out and what the consequences of doing each are
- Set an automated circulation system to purge user personal data when an item is returned
- Delete old web server logs
- On public workstations use boot routines to clear caches, temporary directories, recent history and browsing files
- Ensure hard drives of public workstations are cleaned and recreated at the end of each day
- Delete cookies files or set browsers to reject cookies

Further information
- American Library Association (2005) Privacy Tool Kit
- Australian Library and Information Association (2006) Privacy Policy
- Data Protection Act 1998
- ICO (2007) Sharing personal information: our approach
- IFLA (1999) Statement on libraries and intellectual freedom

Examples of good practice
- Cabinet Office Cross government actions: mandatory minimum measures
- Leicester University About data protection at the University
- Suffolk County Council Privacy and data protection
- Warwickshire Libraries and Information Service
2.3 Data sharing

It is common for personal data to be shared between different departments of an institution or between separate institutions. This is often a result of increased partnership working between different services in order to deliver on a cross-cutting agenda – e.g. tackling deprivation or promoting lifelong learning – and a desire that the same information should be collected only to save the user time. The library service may be the originator of personal data that will be shared (e.g. membership details of a reading group) or a recipient of personal data (e.g. personal details of students from the Registrar’s department of an academic institution). Such personal data may be shared on a regular basis or on an ad hoc or one-off basis. Whatever the case, it is important that the personal data is managed responsibly and in line with the data protection principles (including where appropriate its exemptions). If the benefits of data sharing are to be achieved this must not be at the expense of maintaining public trust and respecting personal privacy.

Checklist

• Does your institution have a code of practice setting out required practice in relation to data sharing? Has the code of practice been endorsed by the Information Commissioner?
• Is it clear which institution/part of the institution ‘owns’ the personal data and has overall responsibility for its responsible management within the terms of the Data Protection Act?
• Is the data provided consistently edited and updated across all partner organisations? Does this include deletion of data when appropriate?
• Have the additional security considerations of providing data across more than one institution or parts of an institution been adequately addressed?
  Do staff know where to refer problems or queries? Are levels of access to the personal data strictly controlled on a ‘need to know’ basis?
  • Are users informed as to how the personal data will be used and where appropriate their permission sought?

Further information


2.4 Personal data security

There have been a number of recent examples of the security of personal data being compromised. Often this has been through the loss or theft of a laptop that contained personal data. Such incidences undermine the confidence of the public in providing personal data and so make the benefits of data sharing – more responsive and personalised services – difficult to achieve. Although there are technical and policy initiatives that can be implemented to improve personal data security (the use of encryption for example), there is also a personal responsibility to be aware of the need to treat personal data responsibly and to demonstrate by your own actions and attitude the importance of treating such personal data with the respect its providers would expect.

Although all personal data should be treated with respect, the Data Protection Act identifies ‘sensitive’ personal data as a specific category of personal data. Typically sensitive personal data would include details on the health or sexuality of an individual, matters pertaining to their religious beliefs or political affiliations, trade union membership, their racial or ethnic background and details about criminal offences, alleged or otherwise, they have committed. Under the Data Protection
Act the threshold of criteria that have to be satisfied before sensitive personal data can be collected is much higher and the need to ensure its security and privacy is also correspondingly higher as the damage and intrusion for the individual can be much greater.

**Memory sticks found in libraries**

Personal memory sticks are commonly used in libraries and there should be a policy in place to deal with found or handed in memory sticks. Below are some examples of policy statements that could be used by an institution:

- Any personal memory stick found in the library will be retained in lost property for xxx days. At the end of this period it will be destroyed and disposed of. No member of staff will view the files stored on the device.
- Any personal memory stick found in the library will be retained in lost property for xxx days. At the end of this period all data will be removed by the IT department and the device will be reused or offered for loan / resale. Files stored on the device will only be viewed by IT staff as is necessary for their secure removal.
- Library / IT staff will attempt to trace the owner of the device by viewing stored files. Where this is possible the device will be labelled with the name of the owner who will be contacted if possible. Where the owner cannot be traced or is uncertain…. [insert a or b as required – removing the final sentence]

**Checklist**

- Has there been a proper risk assessment exercise undertaken recently in regard to information security generally and the security of personal data especially?
- Is there an overall security policy and does it include information and personal data security? Are checks made on its implementation? Does it cover contractors and other third parties? Are security incidents properly investigated?
- Has encryption been considered as a security measure? Does any existing policy cover the use of encryption for mobile devices such as laptops and memory sticks? Is there a policy relating to the secure removal of data before the redistribution of mobile devices within an organisation?
- Does your institution have a policy on dealing with memory sticks found in the library?
- Does the security policy cover the decommissioning of equipment and the deletion of personal data that might be contained on an old hard disk for instance?
- Are you aware of your own responsibilities under the security policy? Are staff trained in their responsibilities?
- Has information security, including personal data security, been covered in the institution’s Business Continuity plans to deal with disaster situations (e.g. major floods, fire, epidemics, terrorist activity)?

**Examples of good practice in the use of encrypted memory sticks**

Leicestershire & Rutland NHS Trust (2009) Guidelines for the use of hardware encrypted memory sticks

University of Leicester Information Security Policy

The University of Manchester Information Handling, encryption & mobile computing
Further information

Information Commissioner’s Office (2010) Our approach to encryption
FSA Guidelines on Responsibility for Customer Data Security (particularly relevant to business/special libraries)
BCS the Chartered Institute for IT/Information Security Awareness Forum (2009) Personal Data Guardianship Code
Information Commissioner’s Office (2007) Data Protection Good Practice Note: Security of personal information
The safe disposal of ICT equipment see The Data Protection Act 1998

2.5 Use of the internet

Internet use - the core issue

Each use of the internet, including use of email, discussion groups and social networks, generates a small dataset in a logfile about the sites visited. It will include traffic data about any communication from its source to its destination and may also contain details of content – full URLs of web pages as opposed to just the address of the relevant web server – and perhaps even individual subscriber details. This data cumulates over a session and a history of use is created in the session logfile. Such logfiles will be created on the PC used and will probably also be recorded elsewhere on the network as well as by the Internet Service Provider (ISP). For the most part this data is generated automatically and not requested by the library. Where libraries register users for internet use (or where internet use is dependent on library membership or registration with the parent institution e.g. a student at a university) it will be possible to link the individual to this data. The privacy and confidentiality of the user could be compromised. Where an individual can be linked to content accessed in this way then it is likely to be regarded as personal data under the terms of the Data Protection Act 1998.

The Privacy & Electronic Communications (EC Directive) Regulations 2003, places restrictions on how logs may be used, the reasons such personal data might be disclosed and it also requires that such logs are protected by appropriate technical and procedural measures.

Internet use - associated issues

It is proper that libraries should do what they can to discourage the viewing of illegal sites. These will often be associated with child pornography, race hate or terrorism. Does the library have an acceptable use policy that all users sign up to? And does this cover users accessing the internet in the library using their own equipment (taking advantage of wi-fi areas provided by the library)?

Internet users may fall victim to the many scams and fraudulent activity that can be found on the web. Most common among these are those seeking to gain information about personal bank accounts. Does the library warn users about such activity? And that the library will not bear responsibility for the consequences of any such scam?

It is also important to note that computers in the library may be used for other types of unlawful or undesirable behaviour – notably hacking, spreading viruses or as an aid to criminal activity. The JISC Legal Information Service provides an informative overview on cybercrime.

Permitted use of the internet may vary according to library or the status of a user. CILIP does not endorse the use of filtering especially for adult users but recognises that a number of libraries do use filtering systems.
especially if it is required by their parent institution. Where filtering is in operation, is this acknowledged publicly? Does the library have an override capability so as to respond to users’ requests to unlock specific sites? Can users appeal against inaccurate filtering? Do some terminals provide unfiltered access?

In some countries ISPs (Internet Service Providers) provide information on personal use to the authorities. In the UK a similar provision has been put into place whereby ISPs have to retain private and personal information including data on email traffic, website browsing histories, internet telephony, and mobile and fixed line telephony for a year. At the moment there is no requirement for ISPs to keep information on the content (e.g. of emails) viewed or sent. See the Data Retention (EC Directive) Regulations 2009 (No 859) vii.

Questions on best practice

Are users warned internet access will leave a thread of data revealing their use of the internet?

Are users informed of the library’s policy of handling this data? In particular – how long is it retained? How closely is it related to individual use and users? What uses are made of the data? What are the arrangements for its eventual destruction?

Are internet use details kept only for a known library use? And are they deleted on a regular basis consistent with any library requirement? Is this policy publicised?

Is the library’s policy on the use of internet usage data published?

Does the library have an acceptable use policy? Is this acceptable use policy in place for those using their own equipment with wifi facilities provided within the library?

All acceptable use policies should be in plain English and in as many languages as appropriate.

2.6 Children and privacy

Children have the same rights as adults under the European Convention on Human Rights (ECHR), which are directly enforceable against public bodies in the UK under the Human Rights Act. This includes a right to respect for private and family life (Article 8) and a right to freedom of expression (Article 10).

The United Nation’s Convention on the Rights of the Child (UNCRC) which applies to all children and young people aged 17 and under also sets out various rights specific to children. This includes:

Article 13: The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice.

Article 16: No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. viii

The UNCRC has been ratified in the UK and has been in force since January 1992. This means that the UK Government is bound to follow policies which conform to children’s UNCRC rights, although children cannot actually take direct action themselves to enforce these rights in the UK. The UNCRC does, however, reinforce the need to respect rights of privacy and freedom of expression in particular where children are concerned.

The Data Protection Act 1998 confers rights on children as well as adults. These rights should only be exercised by another on their behalf if they are not capable of exercising them independently.

Generally if a ‘subject access request’ is received from a parent/carer in respect of a child who is 12 years or older, consent from

vii Original full text, not updated

viii Convention on the Rights of the Child
the child should be sought. If, however, you consider that the child is not of sufficient maturity to understand their rights then their consent is not required. Children are often thought to be sufficiently mature by the age of 12 but they might not be. Also, it might be possible for a younger child to be regarded as having sufficient maturity to exercise this judgement on their own behalf.

A young person who is of sufficient maturity can also make a request (for information held about them) in their own right. Again, this would normally be a young person who is at least 12 years of age.

These can be difficult decisions. They should be taken on a case-by-case basis and taking into account the factors listed in the ICO’s Guide to Data Protection (see Section C – Rights and Exemptions—which includes a section on children).

2.7 Privacy in prison libraries

In the special case of prisons, where internet access is extremely limited, CILIP supports the general principle that internet access should be available to staff and prisoners. This raises some important issues, including the ability of prisoners to prepare information in their legal defence. See Appendix one for background information.

The other important issue in prisons is the question of privacy for prisoners as to their library use. Librarians have a duty to assist the police when this takes the form of an official request for highly relevant information in the urgent investigation of a crime. In some cases where the prison library computer system is integrated with the local authority system, technical reasons may determine that the enquiry may be answered only by an IT unit, for example, within the local authority.

CILIP’s professional ethics stress both confidentiality and the public good. More general enquiries or ‘fishing expeditions’ by the authorities or other professionals such as psychologists may call for careful consideration.

2.8 CCTV in libraries

Use of CCTV raises the question of where the balance of security and privacy should lie. A 2002 study estimated that there are more CCTV cameras per population in the UK than any other country in the world. Use with other emerging technologies, e.g. facial recognition, remote sound recording and RFID raises serious concerns, as does the pervasive ‘because it’s there, we should be able to use it’ attitude. CCTV is also the first and apparently easiest solution available to management but, before its use, it should be clearly established that CCTV is a solution to the problem and that there are not other effective solutions with less impact on privacy.

**Checklist**

- Has there been an assessment of the proportionality of using CCTV in relation to the problem that is being addressed and the impact this will have on people’s privacy?
- Where the system is operated by a public library authority, have wider human rights issues been considered such as the implications of the Human Rights Act 1998?
- Are policies in place covering retention periods and security of data? And are these proportionate and adequate?
- Does the organisation have a procedure for responding to individuals making requests for copies of their own images?
- Are there prominent signs explaining that CCTV is in operation?
- Does your organisation make available its own code of practice (for public authorities, in their publication scheme)?
**Action points**

CCTV and other related devices must be compliant with the Data Protection Act 1998. Notification (and renewal) of the scheme and the name of the data controller needs to be made to the Information Commissioner’s Office (ICO). Operational staff should be trained in and be familiar with the ICO’s ‘CCTV Code of Practice’.

Private sector personnel who operate or monitor public space CCTV systems are subject to licensing by the Security Industry Authority.

Access to data by third parties should be restricted under the terms of the Data Protection Act 1988.

**Further information**

- Data Protection Act 1998
- Human Rights Act 1998
- Information Commissioner’s Office (ICO) (2008 revised edition) CCTV Code of Practice
- ICO Notification under the Data Protection Act 1998
- Security Industry Authority

**Examples of good practice**

- British Library: CCTV systems at the British Library
- Royal Borough of Kensington and Chelsea: Library Service CCTV policy

**2.9 Photography and filming in libraries**

Users should be asked for consent to be photographed and for these images to be published. Particular care is needed in the case of children as there is the possibility of adaptation of images for child pornography and the identification and locating of children at risk.

**Checklist**

- Does the organisation have a clear policy in regard to photography in the library whether for the library/organisation or at the request of others?
- Is the policy accessible and publicised?
- Are staff aware of it and advised on how to implement it?
- Are there any other reasons for concern?

**Further information**

- Museums, Libraries & Archives Council (MLA) Safeguarding Guidance

**Examples of good practice**

- Football Foundation: Photography Code of Practice
- Warwickshire Library and Information Service Child Photographic consent form (Appendix 3)
3 Keeping users informed

This section is indicative of best practice in keeping users informed of library procedures and practices. You can benchmark your own organisation’s practice against this. Libraries are encouraged to make users aware of issues around user privacy and personal data held by the library.

3.1 Providing policies

Policies on customer privacy and protection of personal data should be displayed/made available within library buildings and via the institutional website.

Policies on the use of surveys, feedback forms and any user consultation should be made available to respondents.

Users should also be reminded about personal security – the dangers of publishing their own personal information on the internet, or revealing personal information over the telephone.

3.2 Informing users of the type of data

Personal data should be defined so that users know what data is being kept.

On forms, mandatory information should be explicitly defined.

On forms, non-mandatory information should be explicitly defined, along with details on how users can opt out of this category.

Policies on electronically generated data (e.g. data generated by cookies) should be communicated to users, along with instructions on how to delete cookies, should the user wish to.
3.3 How long the data is kept

Users should be told how long the data will be kept for and how the data will be disposed of after that date.

3.4 What the library/information service does with the data

Users should be made aware of other internal departments, and any external organisations, that may have access to their personal data, and the reasons for that access.

Users should be made aware of exceptional circumstances in which their data may be disclosed to external organisations, such as the police, security services or the Secretary of State, subject to the appropriate legal processes having been followed.

Where possible, users should be informed of the proposed data sharing prior to its taking place but, in any event, as soon as is practicable.

3.5 What the library/information service will do when asked for personal data

Users should be made aware of how the library will respond when an individual asks to see the personal data held on them by the library.

Users should be made aware of how the library will respond when asked by an external organisation, such as the Police, Security Services, GCHQ or the Secretary of State, for personal data on an individual.

Further information

- Data Protection Act 1998
- Freedom of Information Act 2000
- Legal opinion of James Eadie, commissioned by CILIP 2005, on Police access to library user records
- Police and Criminal Evidence Act 1984
- Terrorism Act 2000

Examples of good practice

Warwickshire Library & Information Service – Customer Privacy and Protection of Personal Information

The Law Society’s Data Protection policy (see in particular the Principles and Satisfaction of principles)
It is in the very nature of a library and information service that it handles requests for information. Training in dealing with such requests should be a key component of staff training and development. Privacy issues are central to this process.

All UK organisations must operate within the confines of the Data Protection Act 1998. They will also be subject to other Acts that give the police and security agencies rights to demand access to personal data within specific contexts including the Police & Criminal Evidence Act 1984 and the Terrorism Act 2000. In general, where the disclosure of personal information is required by law or by order of a court, then it is exempted from the non-disclosure provisions within the Data Protection Act – such provision will cover areas such as child abuse. Public authorities listed in the Schedule to the Freedom of Information Act 2000 must also comply with that Act. This includes government departments, local and health authorities, maintained schools, FE institutions, universities and other HE institutions, as well as other listed public bodies including some museums. In Scotland the equivalent is the Freedom of Information (Scotland) Act 2002. Individual CILIP members need to have regard to the Ethical Principles (notably Principle three on access to information and Principle eight on respect for confidentiality and privacy of users).

It is important that the library and information service of any organisation is legally compliant. From time to time it may be necessary to take legal advice on this matter.
The reflective practitioner should think about the following:

- How confident are you and other staff in dealing with requests for personal information about users (or other staff) from:
  - Members of the police or other regulatory or security officials?
  - Other departments within the organisation?
  - Members of the public?
  - External organisations?
  - Other?
- Does your organisation have a policy regarding the handling of such requests?
- Is any policy easily accessible? And properly publicised?
- Have staff been trained in the policy?
- Are you comfortable with the way individual cases have been handled by your organisation? If not, why not?

4.1 Requests from members of the public

It is important to establish whether the request for personal data relates to an individual's own personal data or that of somebody else. In the case of the former the request will constitute a 'subject access request' within the terms of the Data Protection Act 1998. In such cases it will be necessary for the individual to provide proof of identity and also to be clear whether they are interested only in the personal data held by the library and information service or want to know what the whole organisation has. Proper documentation of the procedure is essential.

When a person is asking for personal data about somebody else, then this will have to be looked at under the Freedom of Information Act 2000 (and its Scottish equivalent) where these Acts apply i.e. the public authorities and bodies outlined in section 4 above.

Other organisations will be under no legal obligation to consider supplying such data (and should not do so unless they can comply with the data protection principles restricting disclosure of personal data).

The term, ‘third party data’ is used to describe personal data about someone other than the applicant. In many cases, the request for information (under the Freedom of Information Act or otherwise) can and should be rejected, for example where disclosure of personal data would breach one of the data protection principles. One useful distinction is between ‘public’ personal data (public position held; expenses claimed etc) as opposed to private personal data (home address, marital status etc) with the latter usually being off limits. However a sense of proportion needs to be kept in terms of the risk to the individual (the person whose data is being revealed). Public libraries will have many instances of people wanting ‘third party data’ without posing a real threat – neighbours, for instance, borrowing for a vulnerable person unable to get to the library and wanting to know if ‘they’ve read this one before’. Often the resolution may only be a phone call away to get the permission of the person concerned.

However, in cases of difficulty it should be possible to refer the request to a designated member of staff or specialist unit within the organisation.

**Checklist**

- Does any policy set out how to deal with requests for personal data from members of the public? When their request relates to their own personal data? When their request relates to the personal data of somebody else?
- Is there a designated member of staff or specialist unit to whom more difficult requests can be made?
- Is the process properly documented?
4.2 Requests from other departments or partner organisations

Larger organisations, such as local authorities or universities, will often have a number of departments and many organisations will work in partnership with other bodies. It is important to understand who, in such circumstances, has the right to access the personal data. It is also important to know who ‘owns’ the information and has responsibility for ensuring its accuracy, currency and security.

The starting point for determining these things will be the registered purpose or purposes for which the personal data is being collected as this will determine who will need access to this data. As with personal data used only within the library and information service different members of staff may need different levels of access in order to perform their tasks and this should be reflected in the permissions structure used within the system. It is also important that an individual (the ‘data subject’) is informed as to who does have access to their personal data.

Checklist

• Does any policy of your organisation set out how requests for personal data from other departments within your organisation or partner organisations should be dealt with?
• In cases of difficulty is there a designated member of staff or specialist unit to whom such requests can be passed?
• Are such requests for personal data properly documented to ensure an audit trail?
• Where data is shared between departments or partner organisations have proper arrangements been put in place to ensure that good practice is adhered to in the management and use of such personal data? (See also see section 2.3 on data sharing.)

4.3 Requests from the police and other security agencies

The police and other security agencies have powers to request or demand access to personal data under a number of different statutes. These include, for instance: the Data Protection Act 1998, Terrorism Act 2000, and Police and Criminal Evidence Act 1984. The Regulation of Investigatory Powers Act 2000 may also be relevant (see section 4.5). Each statute sets out a different authorisation procedure. Generally it is important to establish that the police are requesting personal data for a specific purpose (e.g. in regard to a specific arrestable offence) and are not simply on a ‘fishing expedition’. In addition it is important to ensure that the proper authorisation procedure has been followed in each case.

Unless the police have invoked specific powers under one of the Acts there is no general obligation to answer police questions. However, if there are continuing concerns about responding to the police requests when such powers have been invoked, or responding to a court order or notice requiring disclosure of information, then urgent legal advice should be sought.

There are some instances when failure to report a matter to the police can be a criminal offence in itself. Under Section 38B of the Terrorism Act 2000, for instance, it is a criminal offence for a person to fail to disclose, without reasonable excuse, any information which they know or believe might help prevent another person carrying out an act of terrorism or might help in bringing a terrorist to justice in the UK. Where there is doubt about the legal obligations of individuals or an institution legal advice should be sought.
Checklist

• Does any policy of your organisation set out the procedure for dealing with requests for personal data from the police?
• Is there a designated member of staff or unit within the organisation to whom such requests should be referred?
• Are there proper request and authorisation forms to ensure an audit trail for such requests?
• What happens if a request is made outside ‘office hours’?

4.4 Electoral registers

Library staff should be aware of the access restrictions to the full versions of current electoral registers. They can only be consulted under supervision and copied solely by means of hand-written notes. No form of photographic, mechanical or electronic copying is permitted by law. The law also prohibits a library from disclosing any information from full versions of the electoral registers over the phone or in writing or by allowing electronic copying for a period of ten years from the date of issue.

4.5 Covert interception of communications or surveillance

The Regulation of Investigatory Powers Act 2000 may also be relevant. This provides powers for the police and other authorities (including, for instance, local authorities) to mount covert surveillance or interception of communications with proper authorisation. Therefore it is about collecting new information rather than seeking access to existing information but it could involve the use of library systems, facilities or premises.

Further information

• Information Commissioner’s Office (2009) The T!nk privacy toolkit
• CILIP (2004) Ethical Principles for library and information professionals
• Data Protection Act 1998
• Environmental Information Regulations 2004 (full orginal text, not updated version)
• Freedom of Information Act 2000
• Freedom of Information (Scotland) Act 2002
• Legal opinion of James Eadie, commissioned by CILIP 2005, on Police access to library user records
• Police & Criminal Evidence Act 1984
• Terrorism Act 2000
• Regulation of Investigatory Powers Act 2000
5. The law and the privacy of users

Introduction

This section provides an overview of important statutory provision and some of the key bodies responsible for its implementation. This should not be taken to constitute legal advice. CILIP members are strongly advised to recommend that their organisations take appropriate legal advice when necessary. This section may help you to identify those times when such advice is needed, the questions that need to be raised and appreciate some of the complexities that may be involved.

5.1 The key legislation

**Equality Act 2010**

An Act which provides a new cross-cutting legislative framework to protect the rights of individuals and advance equality of opportunity for all; to update, simplify and strengthen the previous legislation; and to deliver a simple, modern and accessible framework of discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society.

**Human Rights Act 1998**

The European Convention of Human Rights is now enforceable through the British courts as a result of the passing of the Human Rights Act. It includes the right to respect for private and family life. The Equalities & Human Rights Commission has responsibility to promote its effective implementation.

**Data Protection Act 1998**

This Act is the main UK legislation ensuring the responsible use of personal data by organisations and is therefore a key piece of legislation underpinning the right to privacy and family life. It sets out the eight data
protection principles and its implementation is overseen by the Information Commissioner’s Office.

This Act seeks to ensure investigatory powers are consistent with human rights. It covers the interception of communications, the acquisition of communications data, surveillance and access to encrypted data.

**Terrorism Act 2006**
This Act creates offences relating to the encouragement of acts of terrorism, and to the dissemination of terrorist publications. It also makes specific provision about how these two new offences are to apply to those providing and using the internet and other electronic services.

**Privacy and Electronic Communications (EC Directive) Regulations 2003**
This mainly covers tele and e-marketing. It also covers the use of calling-line identification, ‘cookies’ and directories. Its implementation is overseen by the Information Commissioner’s Office.

**Public Interest Disclosure Act 1998**
An Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation and for connected purposes. It sets out a framework for public interest whistleblowing and covers workers in all sectors, although some (e.g. volunteers) are not covered.

5.2 Statutory bodies

**Equalities & Human Rights Commission (EHCR)**
The EHRC has responsibility for overseeing the effective implementation of the Human Rights Act 1998. This includes right to respect for private and family life.

**Information Commissioner’s Office (ICO)**
The ICO has responsibility for the implementation of the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003 across the whole of the UK. It also has responsibility for the implementation of the Freedom of Information Act 2000 in England, Wales and Northern Ireland. Scotland has a separate Scottish Information Commissioner dealing with the Freedom of Information (Scotland) Act 2002.

The ICO website includes sections on the rights of individuals and the responsibilities of organisations. The ICO provides an enquiry service but ask that the FAQ section on their website is checked first.

5.3 Other bodies providing advice and information

**JISC Legal Information Service**
“JISC Legal is a free information service offering high quality legal information to further and higher education relating to the use of information and communications technologies” (JISC website). Although its intended audience is higher education and further education staff, most of the information is relevant beyond those sectors.

**Public Concern at Work**
Public Concern at Work (PCaW) is an independent body on public interest whistleblowing. It offers a free confidential telephone advice service to those with whistleblowing dilemmas.
If you are looking for confidential advice on any matters raised in these guidelines or on any other professional issue you are facing, then why not contact CILIP’s Ethics Panel: ethics@cilip.org.uk

See CILIP’s website for further information about CILIP and professional ethics and the Ethics Panel.
Appendix 1

Use of the internet in prison libraries

In the special case of prisons CILIP supports the general principle that internet access should be available to staff and prisoners. There is a political dimension in that while CILIP supports internet access for prisoners as a principle, and undoubtedly prisoners should enjoy basic human rights, there is already a tension between the rights of prisoners and both security and the perceived need for retribution and punishment. Moreover, prisoners do not yet enjoy all the benefits of citizenship, such as the right to vote.

Prison staff and related contractors (education departments and librarians for example) usually have access to a limited range of approved sites, including the BBC site and government sites; with senior staff, in areas where prisoners cannot enter, having full internet access. Up until very recently there has been no access for prisoners to the internet. This has usually been on two main grounds. The first is that it is highly undesirable for the public good that prisoners should have access to information that might make future offending more likely, for example pornographic or violent sites. The second is that internet email could allow prisoners to communicate with their victims, or write to other offenders or anyone else to plan crime. Other methods of communication by prisoners, such as letters, are openly and officially checked by staff to prevent security breaches or risks to staff safety, but this might be impractical or excessively labour-intensive in the case of email.

The disadvantages of lack of internet access for prisoners, apart from the general benefits of access to information to people who are physically restricted, are as follows. Prisoners cannot access information to support educational courses and so have to fall back on the very limited resources of the prison library, or an education department. In particular, Open University (OU) courses, though followed only by a small minority of prisoners, no longer use TV broadcasts and much OU educational material is available online only. Prisoners preparing for release cannot fully equip themselves with ICT skills. A further serious drawback, and one which may be open to challenge, is that prisoners cannot fully access the information needed to prepare a legal case.
Major issues

Prison librarians are working in a special environment, where it is accepted that prisoners, and to some extent staff, do not enjoy all the rights that can be expected in civil society. In general, and particularly in the emergency situation, prison security is paramount, with any challenges to be considered at a later date.

Where there is a conflict between the interests of the prison authority and the librarian/local authority or other agency on the subject of internet access, the librarian has the right to argue the case, and to seek support from the employer (where the library service is contracted to a local authority or other body), or from CILIP.

Prison librarians should co-operate with and support schemes such as Polaris, which are piloting internet access for prisoners on a ‘walled garden’ basis.

If internet access does in future become available in prison libraries, librarians should be careful to make explicit to prisoners any plans to record use, for example information as to which sites have been accessed by a particular prisoner.

Librarians have a duty to assist the police when officers are investigating crime. In some cases where the prison library computer is integrated with the local authority system, technical reasons may determine that the enquiry can be answered only by an IT unit, for example within the local authority.

It is highly desirable that guidelines and detailed plans for collection and disclosure of internet use data should be made in advance by the prison, library staff and any contractor such as the local authority or agency. These could usefully be incorporated in the service level agreement.

CILIP supports the principle of internet access for prisoners, and individual librarians should welcome any future pilots or plans by the government or the prisons to devise creative and safe solutions to the issues raised by this question.

Checklist

- What access are prisoners allowed to the internet? Is this proportionate to the risk represented by the prisoners?
- If prisoners are able to access the internet, do guidelines or a service level agreement set out the parameters for the collection and disclosure of usage data? Are prisoners informed of this?
- Is access sufficient to allow:
  - access to information necessary for prisoners to prepare their defence?
  - support for courses?
  - preparation for release?
- Are some enquiries concerning the personal use of the internet (or library resources generally) really ‘fishing exercises’?

Example of good practice

Polaris: A Ministry of Justice pilot project, Polaris, has been developed in seven London prisons. Polaris stands for Programme for Offender Learning and Resettlement Information Services. Each of the prisons has a Polaris room with a number of computers which have limited access to a number of websites that have been ‘white listed’. The sites, which are accessible through this system, have been security checked and unacceptable links have been removed. Prisoners who wish to use Polaris are risk assessed and have access for timed sessions, under supervision. The future of this project is uncertain, although it is hoped Polaris will continue in some form, according to a briefing by the Prisoners’ Education Trust February 2009.
Appendix 2

CILIP’s User Privacy in Libraries Task & Finish Group

A group was set up by CILIP’s Policy Forum in 2008 to create principles about privacy and develop statements to reflect these principles. The group put together this document to provide guidelines for CILIP members.

Members of the group

Stephen Bury
Head of European & American Collections, British Library

Guy Daines
Director of Policy and Advocacy, CILIP and Secretary to Group (from April 2009)

Angela Donaldson
Honorary Secretary, British & Irish Association of Law Librarians (BIALL)

Ayub Khan
Head of Libraries (Strategy) Warwickshire and CILIP Council Member

Bruce Madge
Immediate Past President, CILIP

Bernard Naylor
Member, CILIP Ethics Panel

Neil Simmons
Vice-Chair, CILIP Prison Libraries Group and Member, CILIP Policy Forum

Barbara Stratton
Senior Policy Adviser, CILIP and Secretary to Group (until March 2009)

Margaret Watson
Chair

Alison Wheeler
CILIP Public Libraries Group and Member, CILIP Policy Forum

Critical friends

John Pateman
Head of Lincolnshire Libraries, member of Information for Social Change

Paul Pedley
Head of Research, Economist Intelligence Unit, information law consultant

Paul Sturges
Professor of Library Studies, Loughborough University

The work of the Task & Finish Group was also supported by Jill Howard (Policy Support Officer) and Jacqueline May (Policy Officer) within CILIP’s Policy & Advocacy Unit.
Appendix 3

Warwickshire Library and Information Service
Child Photographic consent form (Page 1)

Child Photographic Consent Form

Background

- Photographs of children enjoying Library activities or events should not routinely be taken, as this can detract from the primary purpose of the event.
- A number of excellent photographs are available on individual divisional shared files.

Procedure

- To focus on a smaller number of well thought out photo opportunities.
- Usually these will be specially funded and photographs will be taken by professional photographers.
- Where photographs are taken of children the following form must be completed in full by the parent.
- Photographic images must be attached to the appropriate consent form. With all information filed at the local library.
Appendix 3

Warwickshire Library and Information Service
Child Photographic consent form (Page2)

Dear Parent or Guardian,

Warwickshire Library and Information Service has a reputation for producing attractive publications, and has a popular website (www.warwickshire.gov.uk) which shares information and services both in and beyond Warwickshire.

Photographs are a key feature of our publications, display panels and website. They illustrate details of services and represent the people who use them. We constantly need new photographs for our collection. For this reason, we will be soon taking some photographs either in our libraries or at events organised by the Service.

I am asking for your approval to use photos of your child, possibly in a range of publications or on the Warwickshire County Council website. Our policy is that no children will be named and none of the publications will be on sensitive issues. The Library and Information Service is not responsible for photographs taken by photographers from local newspapers.

Please complete the form below and return it to a member of staff. Thank you for taking the time to fill this in.

Yours Sincerely,

Linda Smith
Head of Service - Operations

Name: _______________________________ Relationship to child(ren): _______________________________
(Please Print)

Child(ren) name(s): _______________________________ _______________________________
(Please Print)

Grants permission for the above child(ren) photo(s) to be used by Warwickshire County Council for as long as it is required – please tick all those permission is granted for.

On our website: [ ] In printed publications: [ ] In the broadcast media: [ ]

Signed: _______________________________ Date: _______________________________

Contact Address: _______________________________

Contact Telephone No: _______________________________

Any Comments: _______________________________

Under the Data Protection Act 1998, this information will not be used for any purpose other than that stated on this form.

Discover • Imagine • Learn • with libraries

www.warwickshire.gov.uk/libraries
Appendix 4

List of web links

2. Privacy

2.2 Personal data - the principles

P.7 (iv) IFLA (1999) Statement on libraries and intellectual freedom

(v) CILIP Ethical Principles for library and information professionals

P.9 Further information:
American Library Association Privacy Tool Kit:
http://www.ala.org/ala/aboutala/offices/oif/toolkits/toolkitsprivacy/

Australian Library and Information Association Privacy Policy

Specification for a personal information management system
http://www.bsigroup.com/en/Shop/PublicationDetail/?pid=000000000030175849

Data Protection Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610

Information Commissioner’s Office (ICO) Data Protection Technical Guidance:
Determining what is personal data

ICO Privacy impact assessment handbook

ICO Sharing personal information: our approach


IFLA (1999) Statement on libraries and intellectual freedom

P.9 Examples of good practice
Cabinet Office Cross government actions: mandatory minimum measures

Leicester University About data protection at the University
http://www2.le.ac.uk/offices/itservices/resources/cis/iso/data-protection-and-freedom-of-information/DP_Site/index?searchterm=About%20data%20protection

Suffolk County Council Privacy and data protection
http://www.suffolk.gov.uk/CouncilAndDemocracy/SiteHelp/PrivacyandDataProtection.htm
2.3 Data Sharing

Further information:

2.4 Personal data security

Examples of good practice in the use of encrypted memory sticks
Leicestershire & Rutland NHS Trust (2009) Guidelines for the use of hardware encrypted memory sticks
University of Leicester Information Security Policy
http://www2.le.ac.uk/offices/itservices/resources/cis/iso/pol/pdfs/s16.pdf
The University of Manchester Information Handling, encryption & mobile computing
http://www.its.manchester.ac.uk/media/services/migration/itservices/secure-it/itsecuritypolicies/GP-InformationHandling.pdf

Further information:
Information Commissioner’s Office (2010) Our approach to encryption
FSA Guidelines on Responsibility for Customer Data Security
BCS the Chartered Institute for IT/Information Security Awareness Forum (2009) Personal Data Guardianship Code
http://www.bcs.org/server.php?show=nav.10666

2.5 Use of the internet

Internet use – the core issue
Second para:
Privacy & Electronic Communications (EC Directive) Regulations 2003
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Secondary&PageNumber=43&BrowseLetter=P&NavFrom=1&activeTextDocId=859396

Internet use – associated issues
Third para:
cybercrime
http://www.jisclegal.ac.uk/cybercrime/cybercrime.htm

Fifth para:
Data Retention (EC Directive) Regulations 2009 (No 859)
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Secondary&PageNumber=4&BrowseLetter=D&NavFrom=1&activeTextDocId=3576509
2.6 Children and privacy

P.13 Reference:
Convention on the Rights of the Child
http://www2.ohchr.org/english/law/crc.htm

P.14 Last para
ICO’s Guide to Data Protection

2.8 CCTV in libraries

P.15 Further information:
Data Protection Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610

Human Rights Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=5&BrowseLetter=H&NavFrom=1&activeTextDocId=1851003

Information Commissioner’s Office (ICO) (2008 revised edition) CCTV Code of Practice

ICO Notification under the Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection/notification.aspx

Security Industry Authority
http://www.the-sia.org.uk/home/

P.15 Examples of good practice:
British Library: CCTV systems at the British Library

Royal Borough of Kensington and Chelsea: Library Service CCTV policy

2.9 Photography and filming in libraries

P.15 Further information:
Museums, Libraries & Archives Council (MLA) Safeguarding Guidance

P.15 Examples of good practice
Football Foundation: Photography Code of Practice

3. Keeping users informed

P.17 Further information:
Data Protection Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610

Freedom of Information Act 2000
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=7&BrowseLetter=F&NavFrom=1&activeTextDocId=1876329

Information Commissioner’s Office (2009) Privacy Notices Code of Practice

Legal opinion of James Eadie, commissioned by CILIP 2005, on Police access to library user records
http://www.cilip.org.uk/get-involved/advocacy/information-society/Privacy/Pages/rightsofaccess.aspx
4. How to handle requests for data

P.17 Examples of good practice:
Warwickshire Library & Information Service – Customer Privacy and Protection of Personal Information
http://www.warwickshire.gov.uk/Web/corporate/pages.nsf/Links/50E2AF072BA39727802576DB0057BB4C
The Law Society’s Data Protection policy
http://www.lawsociety.org.uk/documents/downloads/Data%20protection%20policy%20v%201.4%202007-02-06%20.pdf

P.21 Further information:
Information Commissioner’s Office (2009) The Th!nk privacy toolkit
CILIP Ethical Principles for library and information professionals
Data Protection Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610

P.33
Environmental Information Regulations 2004 (full original text, not updated version)
http://www.statutelaw.gov.uk/legResults.asp?LegType=All+Legislation&title=Environmental+Information+Regulations&Year=2004&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=945378&PageNumber=1&SortAlpha=0

Freedom of Information Act 2000
http://www.statutelaw.gov.uk/legResults.asp?LegType=All+Legislation&title=Freedom+of+Information&Year=2000&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1876329&PageNumber=1&SortAlpha=0

Freedom of Information (Scotland) Act 2002
http://www.statutelaw.gov.uk/legResults.asp?LegType=All+Legislation&title=Freedom+of+Information+(Scotland)+Act&Year=2002&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=599972&PageNumber=1&SortAlpha=0

Police & Criminal Evidence Act 1984
http://www.statutelaw.gov.uk/legResults.asp?LegType=All+Primary&title=Police+and+Criminal+Evidence&Year=1984&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1871554&PageNumber=1&SortAlpha=0

Terrorism Act 2000
http://www.statutelaw.gov.uk/legResults.asp?LegType=All+Primary&PageNumber=1&BrowseLetter=T&NavFrom=1&activeTextDocId=1851852
5. The law and the privacy of users

5.1 The key legislation:

P22 Equality Act 2010

P22 Human Rights Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=5&BrowseLetter=H&NavFrom=1&activeTextDocId=1851003

P22 Data Protection Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610

http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=3&BrowseLetter=R&NavFrom=1&activeTextDocId=1757378

P23 Terrorism Act 2006
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=1&BrowseLetter=T&NavFrom=1&activeTextDocId=2321013

P23 Public Interest Disclosure Act 1998
http://www.statutelaw.gov.uk/legResults.asp?LegType=All%20Primary&PageNumber=9&BrowseLetter=P&NavFrom=1&activeTextDocId=1455502

5.2 Statutory bodies:

P23 Equalities & Human Rights Commission (EHCR)
http://www.equalityhumanrights.com

P23 Information Commissioner’s Office (ICO)
http://www.ico.gov.uk/

P23 Scottish Information Commissioner
http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.asp

P23 The ICO website includes sections on the rights of individuals
http://www.ico.gov.uk/for_the_public.aspx
and the responsibilities of organisations

P23 The ICO provides an enquiry service
https://www.ico.gov.uk/Global/contact_us.aspx
but ask that the FAQ section
on their website is checked first.

5.3 Other bodies providing advice and information:

P23 JISC Legal Information Service
http://www.jisclegal.ac.uk/index.html

P23 Public Concern at Work
http://www.pcaw.co.uk/individuals/individuals.htm

6. Ethics Panel

Second para:

P24 See CILIP’s website for further information about CILIP and professional ethics
and the Ethics Panel