



cilip

Chartered Institute of
Library and Information
Professionals



User Privacy in Libraries

Guidelines for the reflective
practitioner

Revised May 2011

Contents

Introduction	4
2 Privacy	7
2.1 Personal data	7
2.2 Personal data – the principles	7
2.3 Data sharing	10
2.4 Personal data security	10
2.5 Use of the internet	12
2.6 Children and privacy	13
2.7 Privacy in prison libraries	14
2.8 CCTV in libraries	14
2.9 Photography and filming in libraries	15
3. Keeping users informed	16
3.1 Providing policies	16
3.2 Informing users of the type of data	16
3.3 How long data is kept	17
3.4 What the library/information service does with data	17
3.5 What the library/information service will do when asked for personal data	17
4. How to handle requests for data	18
4.1 Requests from members of the public	19
4.2 Requests from other departments or partner organisations	20
4.3 Requests from the police and other security agencies	20
4.4 Electoral registers	21
4.5 Covert interception of communications or surveillance	21
5. The law and the privacy of users	22
5.1 The key legislation	22
5.2 Statutory bodies	23
5.3 Other bodies providing advice and information	23
6. CILIP's Ethics Panel	24
Appendices	
Appendix 1 Use of the internet in prison libraries	25
Appendix 2 CILIP's User Privacy in Libraries Task and Finish Group	27
Appendix 3 Warwickshire Library and Information Service Child Photographic consent form	28
Appendix 4 List of web links	30

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.”ⁱ

“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”ⁱⁱ



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

ⁱⁱ Information Commissioner's Office press release (2009)
Making European data protection law fit for the 21st century. Available from:
http://www.ico.gov.uk/upload/documents/pressreleases/2009/rand_report_120509.pdf
[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