

Libraries and privacy

At its May meeting the ALIA Board of Directors endorsed a set of guidelines to assist libraries and library staff to address situations in which police may seek information about library users. In using these guidelines it is important to remember in certain situations it may be appropriate to seek legal advice.

Libraries and privacy: guidelines

Many Australian libraries are developing, or have developed, a privacy policy, which they publicise to their user community.

Principle: 'Libraries and information services shall protect each user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted'

— *Glasgow Declaration on Libraries, Information Services and Intellectual Freedom, proclaimed by the Council of IFLA, 19 August 2002, Glasgow, Scotland.*

These guidelines are intended to assist libraries to develop policies and practices which will enable them to comply with privacy codes, principles and related legislation. It is not intended that they should replace the obtaining of formal legal advice. Libraries may therefore also wish to seek advice from their organisation's legal advisers and lawyers, depending upon their circumstances.

Guidelines for Libraries

A. Personal information

Libraries necessarily need to collect some personal information in order to be able to provide services to their clients. It is important to assess how much personal information you really need.

1. Collect only the personal information as you require to provide services to your clients, but no more than you need to do that. For example, you will need to collect patron details for your registration system, but will not necessarily need to record information such as driver's licence.
2. Ensure that this personal information is available only to relevant staff, used for the purposes for which it was collected and kept only so long as it is absolutely required by the library or the law.
3. Take all reasonable measures to ensure that the personal information is protected against loss, unauthorised use, modification, disclosure or other misuse.
4. Do not disclose or externally publish personal information without consent.
5. Do not require visitors to the library's website to disclose personal information, such as name and e-mail address, before they can access the site. You may however wish to offer visitors the opportunity to register for communication such as e-newsletters.

6. If you collect statistics information on visitors to the library's website, ensure that this information is aggregated for analysis and does not identify visitors personally unless this has been agreed by a visitor.
7. Personal information must not be used in any way relating to direct marketing purposes without prior permission. Ensure that if you have electronic mailing lists, add members only with express permission. Note that under the *Spam Act 2003* it is illegal to send, or cause to be sent, 'unsolicited commercial electronic messages' that have an Australian link.
8. Often libraries use contractors to assist develop or deliver services. Always ensure that their contracts include clauses to cover privacy, especially the handling and disclosure of personal information, and to indemnify the library for any breach by the contractor of their obligations. Where necessary, get contractors to sign separate deeds of non-disclosure of personal information.
9. On your website identify, where practicable, the name of an office or contact within your library to forward enquiries regarding the use and handling of personal information.
10. Publish a statement on privacy on your library's website. Some examples are included below.

B. Requests to disclose personal information

More frequently various authorities, such as the police, are demanding access to information relating to library users. Often such authorities are entitled by law to have access to information, but certain protocols should be observed. The following is intended to assist librarians who have to deal with such demands, while adhering to the principles of librarianship.

1. State and federal laws require libraries to obey privacy laws. (You can search AUSTLII for laws relevant to your jurisdiction: <http://www.austlii.edu.au>.)
2. If police or other law enforcement agencies request the disclosure of personal information:
 - seek advice from your management;
 - seek legal advice if warranted;
 - insist on a search warrant, a court order, or a document signed by an officer of the law enforcement agency and ensure that you receive a copy; and
 - seek advice from ALIA if this is warranted.
3. Do not surrender personal information of clients without a warrant, a court order, or an authoritative document from the law enforcement agency.
4. The warrant, court order, or authoritative document should clearly state what the information is required for, for example an indictable offence in relation to which the information is being sought. This should

ensure that you are sufficiently satisfied that it is reasonably necessary for the enforcement of the criminal law.

5. Where personal information is used for enforcement of the law, the library should include, in the record containing the information, a note of that use.
6. If police confiscate items in conformity with a valid warrant, or court order, insist on receiving a signed receipt for those items with sufficient detail to identify the items accurately.
7. Personal information can also be disclosed where, on reasonable grounds, the library believes that the use of the information is necessary to prevent or lessen a serious and imminent threat to life or the health of the individual concerned.

C. Library policy on actions related to law enforcement

Even though you may never be faced by a situation it is advisable to be prepared, within the context of your organisational framework. The following points might be taken into account.

1. Your library's policies of access and information management should cover the issue of privacy. It may be that this will be within your organisation's privacy policy and procedures rather than a separate library policy, or your library may require a separate policy. Some information resources and examples are listed below.
2. Seek appropriate legal advice on the application of the policy and any contingency plan, or follow the advice provided to your organisation or library.
3. In order to manage effectively ensure that:
 - a copy of the policy and any plan is available to relevant staff;
 - staff are aware of and understand the documents;
 - staff are trained appropriately;
 - appropriate advice and support are available for any situation that may arise, from management, legal support or other organisations.
4. In any actual situation ensure that actions are documented promptly to enable good management for the safety, freedom and privacy of library patrons or staff.

Good practice examples

A number of libraries have privacy statements and policies which provide models that other libraries may find useful:

National Library of Australia, Privacy Statement <http://www.nla.gov.au/privacy.html>.

State Library of New South Wales, Web Privacy Statement <http://www.sl.nsw.gov.au/privacy/>.

University of New South Wales, Privacy Statement <http://www.unsw.edu.au/gen/pd/privacy.html>. ■