Library Council of New South Wales

Privacy Guidelines for NSW Public Libraries

Disclaimer
These guidelines are intended to provide guidance as to legislative requirements regarding privacy and information in NSW, and how these requirements apply to NSW public libraries. NSW public libraries may wish to use the guidelines as the basis for formulating their own privacy policies. The guidelines do not purport to provide a complete account of all possible legislative provisions that might have a bearing on privacy, nor are they able to address all factual scenarios in which privacy issues might arise. Local authorities should, if necessary, obtain independent legal advice regarding any particular privacy issues that arise.

DOCUMENT HISTORY & VERSION CONTROL

Version	Date approved	Approved by	Brief description
1.0	March 2008	Library Council of NSW	The Privacy Guidelines for NSW Public Libraries provide information on privacy matters relevant to providing library services.
2.0	4 December 2018	Public Libraries Consultative Committee	Second release. Reviewed and updated in line with changes in legislation.

These guidelines provide NSW public libraries with information on privacy matters relevant to providing library services.

1. GENERAL PRINCIPLES

Local authorities (councils) are required to comply with legislation that regulates dealings with, and the management of, information. This includes the *State Records Act 1998* (NSW), the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). For this reason, libraries should be aware of terms of these Acts, and ensure that they have systems in place that are consistent, and promote compliance, with these legislative frameworks.

The *State Records Act 1998* (NSW) regulates the retention and disposal of state records by public offices (which includes a council, county council or joint organisation under the *Local Government Act 1993*). One of the main ways in which it does this is by General Retention and Disposal Authorities, which set out requirements for retaining and disposing of records. Of particular relevance to libraries is GA 39 '*General retention and disposal authority: Local Government Records'* ('GA 39'). In particular, GA 39 'Community Services' deals with activities involved in providing library and public information access services.

The PPIP Act and HRIP Act regulate the manner in which agencies (which includes local authorities) deal with personal information and health information. They do this by prescribing Information Protection Principles ('IPPs') and Health Privacy Principles (HPP) with which agencies must comply. These principles regulate the following:

1.1 Collection of personal/health information (see sections 8–11 of the PPIP Act, HPPs 1–4 of the HRIP Act):

- collection must be for a lawful purpose, be reasonably necessary, and must be by lawful means;
- collection must be directly from the individual to whom the information relates;
- individuals must be notified of certain things, including why their information is being collected; and
- information collected should be relevant to the purpose for which its collected, not excessive, accurate, up to date and complete, and should not intrude to an unreasonable extent on the personal affairs of the individual.

1.2 Retention and security of personal/health information (see section12 of the PPIP Act and HPP 5 of the HRIP Act):

- personal/health information should be kept for no longer than is necessary;

- personal/health information should be disposed of securely and in accordance with the requirements for the retention and disposal of personal information; and

- reasonable security safeguards should be taken against loss, unauthorised access, use, modification or disclosure, and all other misuse of personal/health information.

1.3 Provision of access to personal/health information held (see sections 13–15 of PPIP Act and HPPs 6–8 of the HRIP Act):

- reasonable steps must be taken to allow an individual to ascertain what personal/health information the agency holds relating to the individual; and

- individuals must be provided with access to their personal/health information on request.

1.4 Use of personal/health information (see sections 16–17 of PPIP Act and HPPs 9–10 of the HRIP Act):

- an agency must not use personal/health information without taking reasonable steps to ensure information is relevant, accurate and up to date, complete and not misleading; and

- personal/health information should only be used for the purpose for which it is collected.

1.5 Disclosure of personal/health information (see sections 18–19 of PPIP Act and HPP 11 of the HRIP Act):

- Personal/health information should not be disclosed to another person or body unless:

    - disclosure is directly related to the purpose for which the information was collected and the agency has no reason to believe the individual would object;

    - the individual was reasonably likely to be aware, or has been made aware, that information of that kind would usually be disclosed in this manner; or

    - disclosure is necessary to prevent or lessen a serious and imminent threat to life or health.

NOTE

This is a summary of the relevant IPPs and HPPs, and there are a number of exemptions to their operation within the PPIP Act and HRIP Act. Libraries should look to the full terms of the relevant provisions and, where necessary, seek independent legal advice regarding their operation.

2. MEMBERSHIP INFORMATION

2.1 Applications for membership

Under the Library Regulation 2018, the procedure for registration of members, including the term of registration, is to be determined by the local authority. When establishing policies and procedures for membership applications, local authorities must ensure that the collection of personal information in membership applications is consistent with the requirements of the PPIP Act. Processes for applications should:

- only collect personal information that is reasonably necessary for the purpose of providing library services to members, and that the information collected is relevant to that purpose, is not excessive, and does not intrude to an unreasonable extent on the applicant's personal affairs;
- only collect personal information directly from the applicant for membership, unless:
    - the applicant has authorised collection of the information from someone else; or
    - in the case of a person under the age of 16 years, the information is provided by a parent or guardian;
- meet the requirements for notification of applicants, such that applicants are made aware, either at the time of applying or as soon as practicable after of:
    - the fact that their information is being collected;
    - the purposes for which the information is being collected;
    - the intended recipients of the information;
    - whether the supply of information by the individual is required by law or is voluntary, and any consequences if the information is not provided;
    - the existence of any right of access to, and correction of, the information; and
    - the name and address of the agency that is holding the information.

SAMPLE NOTIFICATION
Your personal information is being collected by XYZ Council for the purpose of processing your application for library membership and providing you with library services. The supply of this information is voluntary, however, if you do not agree to provide the information requested, it may not be possible to process your membership application or provide you with some services otherwise available to library members.

< Modify as appropriate > Your information may be disclosed to third parties contracted by Council to provide <information management/technological/IT services> to the library, but only for the purpose of that third party providing those services, and only as permitted by NSW privacy laws <Delete if not applicable>. Your information will not otherwise be provided to a third party unless for law enforcement purposes, or if otherwise required by law.

Membership information is stored <modify as appropriate> on a secure electronic database <and in any other form?>. You have the right to request access to your personal information held by XYZ Council, and may request amendment of your personal information to ensure that it is accurate, relevant, up to date and not misleading. Any inquiries regarding access or amendment to your information should be directed to <insert details>.

2.2 Online member accounts

Establishing online accounts
The same requirements apply with respect to the collection of personal information when members are applying for or establishing online library accounts. In particular:

- information collected should be limited to what is reasonably necessary for establishing an online account and providing services to members, and should not intrude to an unreasonable extent on the personal affairs of individual members.
- notification should be given, as part of the process of establishing the account, regarding the collection of personal information; the purpose for which it is being collected; intended recipients; that the provision of information is voluntary, but that online services may not be able to be provided if information is not provided; the existence of rights to access the information; and the contact details of the library.

Information collected by online accounts
On most occasions where a member logs in to their account, there is likely to be some collection of their personal information. For example, any record of the time that a member logs in, and details of any transaction a member has undertaken would be that member's personal information.
Libraries should ensure they have appropriate measures in place so that information collected by online accounts is managed consistently with requirements of the PPIP Act. Matters to consider:

- information should only be collected in so far as it is reasonably necessary for the purpose of providing library services to members, should be relevant to that purpose, not excessive, and not intrude to an unreasonable extent on the member's personal affairs;
- notification should be provided, preferably each time a member logs in, regarding:
    - the collection of their personal information;
    - the purpose for which it is being collected;
    - any intended recipients of the information;
    - that supply of information is voluntary, but services may not be able to be provided if information is not supplied;
    - the existence of any right of access to, and correction of, the information; and
    - the contact details of the library (or, if information is managed via the council, the council's details)
- There should be appropriate measures and safeguards in place to ensure the security of member's information, and to protect against unauthorised access, use, modification or disclosure.

2.3 Using membership information for mailing lists and surveys

Mailing lists for sending library communications and surveys
Libraries may wish to use members' email and/or mailing addresses for the purpose of sending newsletters, information sheets or other communications regarding library services, or for conducting surveys. So long as these communications are connected with the provision of library services to members, this would be a permitted use of member's personal information under NSW privacy legislation. Nevertheless, it would be prudent to consider implementing the following safeguards:

- notice of the intended use of address details to send information to members could be given at the time at which individuals apply for membership;
- consideration should be given to allow members to either 'opt in' or 'opt out' of receiving some, or all, communications;

In addition, measures should be in place to allow members to update their contact information and to request removal from mailing lists at any time.

Use of third party mail provider
Libraries may use a third-party host to manage or maintain their mailing lists. So long as the third party host simply holds this information, and acts on the instructions of the library, it will be considered to be acting as an agent of the library/local authority and this does not constitute a 'disclosure' of information for the purposes of privacy legislation. Nevertheless, it remains the library's/local authority's responsibility to:

- ensure that member's personal information is managed in a manner consistent with NSW privacy laws; and
- to take such security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, or all other misuse of member's information.

If the third party uses member's data for other purposes, this is likely to be an unauthorised access, use, modification or disclosure of data.

Mailing lists for other communications
Members' email and mailing addresses should not be used for a purpose other than providing library services, unless members have expressly consented to this additional use.

What if council wishes to use our members' information to send emails about upcoming community events or other council functions?
This would be a use of members' information for a purpose other than which it was originally collected. Members' email addresses should only be used for this other purpose where they have consented to receiving this type of additional communication. Libraries may ask for members' consent to this type of additional communication when individuals apply for library membership and/or invite members to 'sign up' for receiving these additional communications.

2.4 Reciprocal membership

Libraries may enter into arrangements for reciprocal memberships. Implementation of these arrangements, and the nature of information that may be shared, depends on the terms of the agreement, and the related membership policies and forms.

What information can be shared between libraries with reciprocal membership?
Except in extraordinary circumstances, personal information about members can only be shared between libraries if:

- the library disclosing the information (the first library) has notified the member that the information in question will be disclosed to the second library, and
- the collection of the information by the second library is reasonably necessary for a lawful purpose directly related to a function or activity of the library, and

- the second library has been authorised by the member to collect that information from the first library.

Exactly what personal information may be shared will depend upon whether the sharing is really necessary in the first place, what type of information is involved, what privacy statement has been given to the person, and what authorisation they have signed. Examples of information that may be appropriate for libraries to share with respect to reciprocal members include:

- confirmation of membership status;
- details of outstanding loans; and
- in limited circumstances, it may be necessary to share information relating to behavioural issues that have impacted on the provision of library services to the client.

What is the recommended process for reciprocal membership applications?
The Local (first) Library will need to give the applicant a privacy statement (see example below). The Reciprocal (second) Library will need the applicant's authorisation to collect their personal information from the first library.

SAMPLE PRIVACY STATEMENT (FIRST LIBRARY) The library may need to supply limited personal information to other libraries if you apply for reciprocal membership of another library. The information provided will usually be limited to confirmation of your membership of our library, and whether or not you have unreturned loans.

SAMPLE AUTHORISATION FOR USE (SECOND LIBRARY) I am already a member of XXX Library. To allow YYY Council to check my suitability for reciprocal membership of *YYY Library*, I authorise YYY Council to collect personal information about me from XXX Library, including whether or not I am a current member, and whether or not I have unreturned loans.

2.5 Membership information of children and young people

As a general rule, libraries should only disclose information about children under the age of 18 (for example, about their membership, borrowing records or overdue books) with the child's consent. The exception to this general rule is where:

- the child lacks the capacity to make decisions about their own personal information. (There is no legally defined age at which children are presumed to obtain capacity to make decisions about their own personal information. While 15 or 16 would be fairly typical, you may form the view that a younger

child has capacity to give or withhold consent to the disclosure of this type of information); and

- you are confident that the person seeking the information (or to whom you wish to disclose the information) is their parent or legal guardian.

2.6 Provision of membership information to law enforcement authorities

While disclosure of membership information to police or law enforcement may be permitted in certain, exceptional circumstances (for example, if such information could assist in ascertaining the whereabouts of an individual who has been reported as missing), in most cases the prudent approach is to ask that a subpoena or court order be issued for the provision of this information.

2.7 Retention and disposal of membership information

GA 39 requires that records relating to applications for membership, including parental/guardian permissions and summary records of borrows, should be retained until administrative or reference use ceases, and then destroyed (GA 39 Community Services, 3.8.6).

3. CIRCULATION RECORDS

3.1 What information can be collected regarding members' loans

Libraries may collect such information regarding members' borrowing history as is necessary for the purpose of providing library services. This would typically include records of what items a member has borrowed, the date on which those items were borrowed, and the date of return of items.

3.2 Sharing borrowing history information as part of reciprocal membership

As discussed at 2.4, information that may be shared between libraries in connection with reciprocal membership will depend on the agreement in place between the libraries, and what consent or authorisation a member has given to information sharing in connection with their reciprocal membership. As a guiding principle, information should only be shared to the extent that it is necessary to do so to allow each library to perform their respective functions.

Example: information about whether a member has any outstanding loans may be considered necessary information to share as part of a reciprocal membership arrangement. However, it would not be necessary to share a list of titles that have previously been borrowed by that member.

3.3 Information regarding children and young people's borrowing histories

See discussion at 2.5 regarding disclosure of information relating to children and young people.

Libraries should be particularly wary of disclosing information about a teenager's borrowing history without seeking the young person's consent. You should only disclose this information to a third party:

- with the young person's express consent; or

- if you determine that the young person lacks the capacity to make the decision for themselves, in which case, disclosure should be limited to the parent or legal guardian.

3.4 Retention and disposal of information relating to loans

GA 39 provides that records of temporary loans should be retained for a minimum of two years after the loan has been completed, and then may be destroyed (GA 39 Community Services, 3.8.4).

4. RECORDS RELATING TO RESEARCH SERVICES AND ENQUIRIES

Where records of reference inquiries include identifying information of a member, they constitute personal information, and should be managed in accordance with the IPPs outlined at 1 above.

Records of research services and enquiries are state records and should be retained until administrative or reference use ceases, and then destroyed (GA 39 Community Services, 3.8.7).

5. COMPUTER AND INTERNET USAGE

5.1 Booking records

Where booking records for internet/computer use include identifying details of members, they constitute personal information and should be managed in accordance with the IPPs outlined at 1 above.
Booking records are also State records, and should be retained for a minimum of 2 years after action has been completed, and then may be destroyed.

5.2 Inadvertent collection of personal information by members' internet usage

A library is only responsible for personal information that it collects and holds. Libraries should be aware of the possibility that they are inadvertently collecting personal information about members who are using public computer terminals, for example, by the operation of anti-virus software, creation of automatic backup tapes and cookies. To avoid or minimise this inadvertent collection, public-use PCs should be configured, so far as possible, not to collect personal information about users. Libraries may also consider displaying prominent signs visible to users of public terminals, reminding them to take steps to prevent the risk of their information being accessed by later terminal users. Such warnings could also, or alternatively, be displayed on the computer terminals themselves, as part of a log-in process.

See also *Library Council of NSW, Internet Policy Guidelines*

6. HOME LIBRARY SERVICE

6.1 Collection of information about next of kin/emergency contacts and health information

Libraries may collect information about a members' next of kin and/or emergency contact, so long as that information is considered to be **reasonably necessary** for the purpose of providing library services to that member. It may also be necessary to collect members' health information, where this is necessary for the provision of

library services, for example, information about special needs arising due to physical or mental conditions or ailments.

Information about emergency contacts **should be collected directly from the member** where the member has the capacity to make decisions about the handling of their own personal information (for example, if the client is physically housebound, but mentally capable). The member should be able to update these details, or change their nominated contact at any time.

Where the member has **temporary or impending incapacity** to make decisions about the handling of their own personal information (for example, if the member is in the early stages of dementia), the member should be asked to:

- provide the contact details of an appropriate contact person, to be contacted in case of some emergency, and
- nominate a 'substitute' decision-maker in the need arises in the future, to assist in nominating books to be borrowed for the member, and accepting responsibility for returning books on time.

The member may wish to nominate the same person for both roles, or two different people. The member should be able to change their nominated contact person and/or substitute person at any time.

Where the member already and **permanently lacks the capacity** to make decisions about the handling of their own personal information (for example, if the member has advanced dementia), then the 'next best person' should be approached on their behalf. See the Information and Privacy Commission's Best Practice Guide, *Privacy and People with Decision-making Disabilities*, for detailed guidance on determining capacity, who to approach and in what circumstances. The nominated or chosen 'substitute' decision-maker should agree in writing to be the contact person in case of some emergency, as well as to assist in nominating books to be borrowed, and accepting responsibility for returning books on time.

6.2 Disclosure of member's borrowing history

If the member (or, if the member lacks capacity, their substitute decision-maker) has consented, the member's preferences and history of items borrowed could be disclosed to those library staff or volunteers involved in choosing items for that member. The consent form should be incorporated into the application form when first joining the service.

7. COMMUNITY INFORMATION DIRECTORIES

Information collected by libraries for community information directories may contain personal information. Accordingly, it is important to observe the IPPs in the collection and management of this information.

In particular, at the point at which this information is collected, the library should ensure that:

- the information is being collected directly from the individual concerned;
- the information collected is reasonably necessary for the purpose for which it is collected (that is, inclusion in the directory), and does not intrude to an unreasonable extent on the individual's personal affairs

  Example: it would only be necessary to collect the individual's business address for the purposes of a community information directory. There would be no need to collect their residential address, and doing so would constitute an intrusion on their personal affairs.

- notification is given to the individual, at the time at which their information is collected, of:
  - the purpose for which the information is being collected – that is, inclusion in a community information directory;
  - that the directory will be published, such that any information provided will be made publicly available;
  - that the provision of information and participation in the directory is voluntary; and
  - identifying avenues for access, updating and correcting information provided.

It would also be prudent to confirm at the time that the information is collected that the individual providing the information consents to the inclusion of their information in the community directory, and its publication (whether in print form, online or both).

8. LOCAL STUDIES COLLECTIONS – PERSONAL PAPERS

Information kept in library collections is exempt from the requirements of the PPIP Act*:* see Privacy and Personal Information Protection Regulation 2014*,* clause 5.

However, it is advisable that libraries have their own policy/procedure about disclosing information from personal papers which will identify material of a sensitive/confidential nature not for release until a specified year. Often there are stipulations at time of deposit that must be adhered to.

9. CCTV AND OTHER FILMING ON LIBRARY PREMISES

9.1 Installation of CCTV

Where CCTV is installed on library premises, the collection and management of CCTV footage must comply with the requirements of the PPIP Act and (insofar as cameras will capture images of library employees) the *Workplace Surveillance Act 2005* (NSW)*.*

CCTV can be installed in most public areas or in staff areas, but may not be installed in bathrooms or change rooms. In considering placement of cameras, regard should be had to:

- the **purpose** for which footage is to be collected — remembering that under the PPIP Act, that purpose must be a lawful purpose directly related to a function or activity of the agency.

  It has been accepted that councils have a crime prevention function, and that use of CCTV is consistent with that function. Related lawful purposes may include ensuring the safety of library patrons, and preventing damage to library property; and

- ensuring that cameras only collect information that is '**reasonably necessary'** for that purpose.

  Example: it may be appropriate to place cameras so as to obtain high views of library premises, and also areas that are out of sight and require additional monitoring, such as library stacks. It would not be reasonably necessary to focus cameras on specific computer monitors and/or keyboards in a manner that would capture computer use of individual members.

9.2 CCTV notification requirements

Where cameras will capture images of library employees, it is prudent to ensure compliance with the notification provisions of the *Workplace Surveillance Act* (even if the purpose of the cameras is not surveillance of employees). These include signs at each entrance of the premises, ensuring the cameras are clearly visible, and providing written notice to staff at least 14 days prior to installation.

As the cameras will also collect 'personal information' of library patrons, it is also necessary to comply with notification requirements under the PPIP Act. This might be achieved by the prominent display of signs on library premises providing notification:

- that the premises are monitored by CCTV;
- the purpose for which footage is collected;
- the intended recipients of the information (for example, law enforcement agencies); and
- contact details for any inquiries regarding CCTV footage and how it may be accessed.

9.3 Providing CCTV footage to police

Libraries may only provide CCTV footage to the NSW Police Force, or other law enforcement agencies, in circumstances permitted by the *Workplace Surveillance Act,* PPIP Act or some other law.

Under the *Workplace Surveillance Act,* surveillance footage of employees may only be provided to a law enforcement agency:

- for use in connection with the detection, investigation or prosecution of an offence;
- for a purpose that is directly or indirectly related to civil or criminal proceedings; or
- where disclosure is reasonably believed to be necessary to avert an imminent threat of serious violence to persons or of substantial damage to property.

The *Privacy and Personal Information Protection Regulation 2014* allows local authorities to provide CCTV footage by way of live transmission to the NSW Police Force. Otherwise, under the terms of the PPIP Act footage may only be provided to police where:

- required by subpoena or by search warrant or other statutory instrument, or
- in connection with proceedings for an offence or for law enforcement purposes, or
- to a law enforcement agency for the purposes of ascertaining the whereabouts of a missing person, or
- if it is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed, or
- the library believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of any person, or
- if the library is lawfully authorised or required to disclose the footage under another Act.

9.4 Providing CCTV footage to other third parties

CCTV footage collected by local authorities is 'government information' and, as such, any person may apply to access it under the *Government Information (Public Access) Act 2009* (NSW). Any such application for access should be made to, and determined by, the local authority.

Libraries may only disclose CCTV footage to third parties in very limited circumstances, where such disclosure is directly related to the purposes for which the footage is collected, and appropriate notification has been given that such disclosure would usually occur.

Example: Can I show CCTV footage to a school principal in order to identify students who are depicted in footage damaging library property?

Disclosure to the principal in this scenario would be consistent with the purpose of collecting footage for crime prevention, and to protect library property. However, unless there were signs around the library that gave appropriate notice that a disclosure of this kind would *usually* occur, it would not be permitted under the PPIP Act.

If the library wishes to identify students who have committed an offence, the more appropriate course would be to refer the matter to the NSW Police.

9.5 Other filming or photography on library premises

Libraries should obtain consent before taking photographs of clients on library premises, and using photographs in publicity, the library's website or social media. It is prudent to obtain consent in writing. In circumstances where it is only possible to obtain verbal consent, make a contemporaneous file note of consent having been given.

Where the photograph is of a child, consent should be sought from their parent or guardian.

9.6 Display of photographs or stills from CCTV footage

It may be necessary to display photographs or stills from CCTV footage of individuals, for example, where they have been excluded from library premises. So far as possible, such photos should be displayed in areas that are reserved for staff, and should not be in an area that is generally visible to members of the general public that are using the library.

10. REQUESTING PRODUCTION OF IDENTIFICATION

Generally, staff may request identification from library members for membership applications, using library equipment, borrowing rare or valuable items or when library rules have been violated. However, in doing so, the library must observe the IPPs and consider the following:

- it is reasonable necessary in the circumstances to identify the person, for example, this may be necessary for the use of library equipment;
- the purpose for which the identification information is being collected is described in a privacy statement or notification, for example, on the application form, borrowing or equipment hiring form;
- Government-issued identification numbers (such as drivers licence numbers, Medicare numbers etc) are not copied or adopted as part of member records unless it is necessary to do so; and

- any copies taken are held securely, and securely destroyed as soon as equipment/materials are returned without damage.

11. DIGITAL INFORMATION

11.1 Mobile apps

Libraries must also observe the IPPs when designing and managing mobile applications for smartphones, tablet computers and other mobile devices. These raise issues that need to be considered as part of the app's design and implementation. In particular, consideration should be given to the following:

- The app should only require provision of such personal information as is reasonably necessary to perform the function or provide the service for which the app is designed.

  Example: while it may be necessary to collect personal information such as a member's name, membership number and email address when setting up an account, it is questionable whether it would be necessary to also collect the member's date of birth.

- Ensure there is adequate transparency regarding the collection of information and privacy so as to ensure compliance with the relevant IPPs. In particular, privacy practices could be communicated to users before they download the app. Consideration should also be given to designing the app interface so that users are alerted to when they are making decisions regarding their personal information and privacy by use of sounds or colour;

- Users should be able to refuse to update an app; to easily deactivate or delete an app; and to update their personal information stored by the app;

- Libraries should ensure they have sufficient technical and organisational measures in place to protect personal information collected.

11.2 Cloud computing

Libraries must have regard to IPPs and HPPs where personal and/or health information is transmitted or stored using cloud computing services. These are matters that generally should be considered as part of the procurement process, and when entering into contractual arrangements with cloud service providers. In particular, consideration should be given to:

- whether the transmission of information will constitute a 'disclosure' of personal/health information to a cloud service provider;

- what safeguards and measures are available for protecting against misuse, loss, or unauthorised access, use or alteration of data;

- ensuring there are avenues for accessibility to the data by the agency (and, where the individual requests access to that information, that it is possible for the agency to respond to that request);

- what is the legislative environment and governing data laws in the location where the data will be stored;
- arrangements for authorised data retention and disposal; and
- making arrangements for who has control of the data at the end of a contract.

Where a contracted cloud service provider simply holds data, and acts according to the library's instructions, then it will usually be considered to be acting as an agent of the library, and 'disclosure' of information will not have occurred. However, if the cloud service provider uses the data for some other purpose, this may constitute unauthorised access, use, modification or disclosure of the personal information.

See also: the NSW Government Cloud Policy.

12. ASSISTING MEMBERS WITH FILLING OUT FORMS

Members may ask library staff to assist them with tasks not directly related to their library membership, such as filling out forms. It is a matter for libraries and their staff as to whether they are willing to provide this type of assistance to members. In providing this assistance, staff should be mindful of the obligations imposed by privacy legislation.

Where a client has expressly asked for assistance with filling out a form, they may be taken to have consented to the staff member dealing with their information in the manner required. So, for example, any 'collection' of the client's information in order to fill in the form would be permitted, as it would be with their consent. However, where the information does not relate to the provision of library services, there should be no need for the library to retain a copy of that information, or use it for any other purpose.

Definitions:

GA 39	General Retention and Disposal Authority 39 *General retention and disposal authority: Local Government Records,* issued under the *State Records Act 1998 (NSW),* authorise the retention and disposal of records common to local government
Health Information	Includes information or an opinion about the physical or mental health or disability of an individual. See full definition in section 5 of the *Health Records and Information Privacy Act 2002* (NSW)
HPPs	Health Privacy Principles under the *Health Records and Information Privacy Act 2002* (NSW)
HRIP Act	*Health Records and Information Privacy Act 2002* (NSW)
IPPs	Information Protection Principles under the *Privacy and Personal Information Protection Act 1998* (NSW)
Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. See full definition in section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW)
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)