

# Supreme Court of Queensland Library Privacy Plan

---

## Introduction

The Queensland Government privacy scheme was introduced to establish a framework for the responsible collection and handling of personal information in the public sector. The scheme is intended to give effect over time to the Commonwealth Government public sector Information Privacy Principles (IPPs) contained in the Commonwealth *Privacy Act 1988* in the Queensland public sector.

Information Standard 42 requires Government agencies to comply with the eleven Information Privacy Principles, governing the collection, storage, use and disclosure of personal information. The Supreme Court Library has developed privacy plans to give effect to these IPPs.

## Scope

Information Standard No. 42 requires personal information to be managed in accordance with a set of IPPs adapted from the Commonwealth Government public sector IPPs contained in the Privacy Act 1988 (Cth). It should be noted that the requirement for agencies to comply with the Information Standard and guidelines is administratively based. This means that:

- where conflicting requirements exist, any legislative requirements will supersede compliance with the Information Standard;
- compliance is subject to any existing outsourcing arrangements, contracts and licenses. Any future outsourcing arrangement, contracts and licenses will be expected to comply with Information Standard 42. Where any existing outsourcing arrangements, contracts or licenses contemplated a future privacy regime (for example, where privacy clauses were written into a contract or license in anticipation of a future privacy regime) it may be possible to re-negotiate these terms.

## Legislative Requirements

The following legislation will supersede the Information Privacy Principles:

*Supreme Court Library Act 1968*

*Supreme Court Library Rules 1987*

*Freedom of Information Act 1992*

## Personal Information

Information Standard 42 is concerned with “personal information”. This is defined in the Information Standard as being:

“Information or an opinion (including information or an opinion forming part of a database), whether true or not, whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.”

Personal Information may be contained in (but is not limited to) the following:

- documents;

- databases;
- spreadsheets;
- photograph of an individual; or
- video tape of an individual.

Personal Information found in the following areas is not covered by the Information Privacy Standard:

- a generally available publication eg. newspaper;
- anything kept in a library, art gallery or museum for the purpose of reference, study or exhibition;
- those public records to which the public has a right of access; for example registers open to public inspection and copying; or
- letters or other articles in the course of transmission by post.

## **Classes of Personal Information**

### **Employee Personnel Records**

The Library collects, stores and uses personal information about current, former and prospective employees. These records are maintained for the purpose of administering human resource management functions, including personnel, payroll and recruitment.

Personnel and Payroll records may include details about:

- attendance and overtime
- leave applications
- medical records
- salary and superannuation
- employee bank account details
- employee tax file numbers
- personal history files
- education
- employment history
- contracts and conditions of employment
- disciplinary action
- compensation claims
- employee phone numbers and addresses
- next of kin contact details

Recruitment records may include details about:

- personal history files
- education
- employment history
- contact phone numbers and addresses

- referee contact details
- referee checks
- interview rating and performance

The information contained in these records is stored securely in both electronic and print files. The following Library staff have access to these files: the Librarian, personnel management staff, supervisors, payroll officers and the individual to whom the record relates.

Personnel records are stored as required to meet audit and financial requirements. Recruitment records, relating to non-employees, are stored for a one year period before being destroyed.

Certain types of personnel information may be disclosed to: the Australian Taxation Office, QSuper and auditors, where legally required.

Individuals can obtain details of specific record handling practices and information regarding access to their personal files by contacting the Librarian (07) 3247 4373.

### **Client Records**

The Library collects, stores and uses personal information about clients. These records are maintained for the purposes of managing the circulation of Library materials and providing a flexible range of information services. These information services include reference, document delivery and research services, which often require the collection of specific details and background information about legal matters and proceedings.

Circulation records may include the following details:

- name
- contact details
- occupation
- current borrowing details

Information services records may include the following details:

- name
- contact details
- occupation
- transaction history (including details / history of document and research requests in relation to legal matters)
- details outlining the nature of reference / research queries
- banking details

Client records are stored in both electronic and print media and are accessible by the following staff, subject to operational need: the Librarian, Client Services staff and accounts managers.

Patron records are established in an electronic database for an initial one year period and are reviewed annually. Inactive patron records are deleted. Information Services records are stored as required to meet audit and financial requirements.

Information contained in these records will not be disclosed to any third parties without the prior consent of the individual concerned, except where required for financial audit purposes.

Clients wishing to obtain further information about record handling practices and information regarding access to their personal records should contact the Librarian (07) 3247 4373.

### **Vendor Records**

The Library collects, stores and uses personal information about vendor staff for the purposes of liaising, negotiating and purchasing materials and services for the Library. These records contain publisher and vendor contact details, which allow the Library to conduct regular business transactions with other organisations.

Vendor records may include the following details:

- name
- contact details
- occupation (including level of seniority)
- banking details

These records are contained in electronic and print media and are accessible by the following staff, subject to operational need: the Librarian, section managers and accounts managers.

Vendor records are stored as required to meet audit and financial requirements.

Personal information contained in these records will not be disclosed to any third parties without the prior consent of the individual concerned, except where required for financial audit purposes.

Vendor staff wishing to obtain further information about record handling practices and information regarding access to their personal records should contact the Librarian (07) 3247 4373.

### **Administrative Registers**

The Library collects, stores and uses personal information contained in contact registers. These registers are maintained for the purposes of communicating with the legal and broader communities, allowing the Library to promote community services and convey relevant information to specific client groups.

Registers kept by the Library include:

- Visitors' Books (for both the Library and special exhibits)
- After-hours access register
- Invitation lists
- Client contact directories

Administrative registers may contain the following details:

- names
- contact details
- occupation
- professional details
- attendance details (for the Library and specific events)

These registers are stored in both electronic and print media. Please note that access to details in the above registers is restricted to the purpose for which the register is kept, unless legislation or regulation provides otherwise.

Visitors to the Library are required to enter their name, address and signature into a designated visitors' book, in accordance with the *Supreme Court Library Rules*. Visitors' books for special exhibits are kept only for statistical and feedback purposes and do not require the entry of a person's full name or contact details.

A register of persons authorised to access the Library outside of normal opening hours is kept for security and statistical purposes.

Invitation lists and contact directories are registers kept by staff to facilitate an efficient and effective means of communicating with large groups of individuals. Invitation list details are used only for the purpose of notifying interested parties of special events and activities. Client registers are used to communicate information about the Library and its services to relevant groups of clientele.

These registers are not shared or made available to any third parties and are accessible by the following staff members: the Librarian, section managers, and secretarial and administrative staff.

Individuals wishing to obtain further information about record handling practices and information regarding access to their personal records should contact the Librarian (07) 3247 4373.

### **Financial Management Records**

These records are maintained for the purpose of processing and managing expenditure and revenue within the Library. The records contained in the Library's financial management system incorporate personal information relevant to other classes of information identified within this Privacy Plan.

Personal information contained in the employee; client; and vendor categories may also be duplicated in the print and electronic financial records stored by the Library. These records are kept as required for audit and financial purposes.

The following Library staff have access to the information contained in the financial management system: the Librarian, accounts managers and section managers.

Individuals wishing to obtain further information about record handling practices and information regarding access to their personal records should contact the Librarian (07) 3247 4373.

### **Information Systems Records**

The Library's information technology and information management systems enable the efficient processing and storage of information, spanning the Library's range of core business activities. Electronic data sources are maintained within the Information Systems structure, providing Library staff with efficient and streamlined access to information. These electronic data sources contain the majority of personal information records identified within this privacy plan.

Information stored in electronic media is protected by the allocation of usernames and passwords to individual staff members. The Library's Information Technology Officer has administrative rights over the Information Systems.

Individuals wishing to obtain further information about record handling practices and information regarding access to their personal records should contact the Librarian (07) 3247 4373.

## **Existing Contracts and Licence Agreements**

The Supreme Court Library enters into contractual arrangements with a variety of external parties for the supply of goods and services. These contractual arrangements have been in existence prior to the Library's requirement to comply with the information privacy principles. When existing contracts are renewed, they will be reviewed and amended to comply with the privacy principles. Any new contracts will also comply with the privacy principles.

## **Procedure to Gain Access to Personal Information**

The Queensland Government privacy scheme includes rights of access and correction for individuals where personal information is collected, stored and used by the Library.

*Information Privacy Principle 6* entitles a person to access any record containing their personal information, except where access is restricted by law. *Information Privacy Principle 7* entitles that person to seek an amendment to any record containing their personal information, where that information is misleading, irrelevant, not up-to-date or incomplete.

These rights are limited to existing rights under the *Freedom of Information Act 1992*.

Individuals wishing to gain access or seek amendment to their personal records should contact the Librarian (07) 3247 4373.

## **Review Procedure**

If an individual believes that their personal information has not been dealt with in accordance with an IPP they may make a complaint to the Library seeking an internal review. A request for an internal review must be made in writing and must be made within six months from the date when the breach was suspected to have occurred.

Written requests should be forwarded to:

The Librarian  
Supreme Court of Queensland Library  
PO Box 15019  
CITY EAST Q 4002

Requests for review will be acknowledged in writing within 14 days from the date on which the application was received, and the Library will endeavour to process the request within 60 days from the date on which the application was received. Applicants will be advised in writing of the outcome.

If an applicant does not agree with the Library's decision they may request further internal review. The Librarian will arrange for an internal review to be carried out by a more senior officer who has not previously been involved in the matter. This will be done within 45 days. The Librarian will provide a response in writing to the individual.

## Implementation Schedule

The Library has developed the following schedule, with a view to reviewing procedures annually.

Objective	Implementation
<b>1. Foster workplace commitment to privacy principles and conduct staff training on procedures and responsibilities</b>	<p>Advise current staff of privacy principles and responsibilities and provide continued updates as more advanced information handling and storage procedures are developed.</p> <p>Provide IPP documentation to section managers.</p> <p>Incorporate privacy policy and guidelines in training for new staff members.</p> <p>Provide all staff with the name of the Library's privacy contact officer.</p>
<b>2. Review existing policies and guidelines</b>	<p>Review policies, procedures and guidelines relevant to the responsible collection, storage and handling of personal information.</p> <p>Review current timeframes for the retention and disposal of these records.</p>
<b>3. Review the security of datasets containing personal information</b>	<p>Review the security of information stored in print and electronic media to ensure compliance with IPPs.</p>
<b>4. Review all notices, request forms, surveys etc concerning the collection of personal information</b>	<p>Modify forms and notices to ensure compliance with IPPs.</p>
<b>5. Notify clientele of the Library's compliance with IPPs</b>	<p>Review and update documents to assure clients of the Library's commitment to maintaining the privacy and security of personal information.</p>
<b>6. Notify vendors of the Library's compliance with IPPs</b>	<p>Review and update documents to assure vendor staff of the Library's commitment to maintaining the privacy and security of personal information.</p>
<b>7. Develop complaint handling procedures</b>	<p>Develop guidelines for dealing with complaints and inform staff of handling and resolution procedures.</p>
<b>8. Develop privacy policies and guidelines</b>	<p>Develop specific sets of guidelines applicable to staff, clients and vendors. Issue these guidelines to staff and via Library service points.</p>
<b>9. Conduct an annual review of policies and procedures</b>	<p>Review the content of privacy policies and guidelines and update as necessary. Monitor adopted procedures and security measures with the Library.</p>

## Appendix A

### Summary of Information Privacy Principles

#### Policy Statement

Personal information held by Queensland agencies must be responsibly and transparently collected and managed (including any transfer or sale of personal information held by agencies to other agencies, other levels of Government or the private sector) in accordance with the requirements of the Information Privacy Principles.

#### Policy Principles

Agencies must comply with eleven IPPs, which govern how personal information is collected, stored, used and disclosed.

The IPPs deal with the following: -

- Principle 1: Manner and purpose of collection of personal information;
- Principle 2: Solicitation of personal information from individual concerned;
- Principle 3: Solicitation of personal information generally;
- Principle 4: Storage and security of personal information;
- Principle 5: Information relating to records kept by record-keeper;
- Principle 6: Access to records containing personal information;
- Principle 7: Alteration of records containing personal information;
- Principle 8: Record-keeper to check accuracy, etc., of personal information before use;
- Principle 9: Personal information to be used only for relevant purposes;
- Principle 10: Limits on use of personal information;
- Principle 11: Limits on disclosure of personal information.

#### **Collection of Personal Information (IPPs 1-3)**

##### **Information Privacy Principle 1**

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

- (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
- (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

##### **Information Privacy Principle 2**

Where:-

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:-

- the purpose for which the information is being collected;
- if the collection of the information is authorised or required by or under

law, the fact that the collection of the information is so authorised or required; and

· any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

### **Information Privacy Principle 3**

Where:-

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:-

· the information collected is relevant to that purpose and is up to date and complete; and

· the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

### ***Storage and Security (IPPs 4-5)***

#### **Information Privacy Principle 4**

A record-keeper who has possession or control of a record that contains personal information shall ensure:-

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

#### **Information Privacy Principle 5**

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the record-keeper has possession or control of any records that contain personal information; and

(b) if the record-keeper has possession or control of a record that contains such information:-

· the nature of that information;

· the main purposes for which that information is used; and

· the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the State that provides for access by persons to documents.

3. A record-keeper shall maintain a record in the form of a privacy plan setting out:-

- the nature of the records of personal information kept by or on behalf of the record-keeper;
- the purpose for which each type of record is kept;
- the classes or types of individuals about whom records are kept;
- the period for which each type of record is kept;
- the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
- the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall make the record maintained under clause 3 of this Principle available for inspection by members of the public.

### ***Access and Alteration (IPPs 6-7)***

#### **Information Privacy Principle 6**

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the State that provides for access by persons to documents.

#### **Information Privacy Principle 7**

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:-

- is accurate; and
- is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the State that provides a right to require the correction or amendment of documents.

3. Where:-

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provision of a law of the State;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

### ***Accuracy (IPP 8)***

#### **Information Privacy Principle 8**

A record-keeper who has possession or control of a record that contains personal

information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

### ***Use and Disclosure (IPPs 9-11)***

#### **Information Privacy Principle 9**

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

#### **Information Privacy Principle 10**

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:-

- (a) the individual concerned has consented to use of the information for that other purpose;
- (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- (c) use of the information for that other purpose is required or authorised by or under law;
- (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

#### **Information Privacy Principle 11**

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:-

- (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
- (b) the individual concerned has consented to the disclosure;
- (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
- (d) the disclosure is required or authorised by or under law; or
- (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.