

Queensland Audit Office

Privacy Plan
January 2009



Contents

Foreword	3
1. Introduction	4
2. Personal information	4
2.1 Exemptions to non-disclosure of personal information	4
3. Acts that effect the Queensland Audit Office	4
4. Types of personal information held by the Queensland Audit Office	5
4.1 Client records	5
4.2 Contract auditor records	6
4.3 Employee personnel records	6
4.3.1 Personnel and payroll	6
4.3.2 Recruitment	6
4.3.3 Other records	7
4.4 Financial management system information	7
4.5 Information systems personal information	7
4.6 Office of the Auditor-General and other QAO records	7
4.7 Alumni records	8
5. Existing contracts, licences and outsourcing arrangements	8
6. Review schedule	9
7. Procedure to access and amend personal information	9
8. Complaint and review procedures	9
9. Information Privacy Principles	10
Appendix A – Summary of information privacy principles	11
Information Privacy Principle 1	11
Information Privacy Principle 2	11
Information Privacy Principle 3	12
Information Privacy Principle 4	12
Information Privacy Principle 5	12
Information Privacy Principle 6	13
Information Privacy Principle 7	13
Information Privacy Principle 8	13
Information Privacy Principle 9	13
Information Privacy Principle 10	13
Information Privacy Principle 11	14

Foreword

The Queensland Audit Office is committed to maintaining the privacy and confidentiality of personal information and will adhere to the Information Privacy Principles when collecting, using, disclosing, securing and providing access to private information.

The QAO Privacy Plan sets out the steps QAO has taken and will take to ensure our compliance with *Information Standard No 42 – Information Privacy*.



Glenn Poole
Auditor-General

1. Introduction

The Queensland Government has established a privacy regime to protect personal information held by Queensland public sector agencies in the delivery of Government services and the conduct of their business. The Queensland Government adopted the national information privacy principles (IPPs) and these have been included in *Information Standard No 42 - Information Privacy*. The standard requires agencies to develop and implement privacy plans to give effect to these information privacy principles which deal with the handling, use and disclosure of personal information. A copy of the information standard can be accessed at <http://www.qgcio.qld.gov.au>.

The Queensland Audit Office's (QAO) Privacy Plan outlines the types of personal information collected and kept by QAO. Our plan also provides guidance on the requirements of the information standard and strategies that have been implemented to ensure compliance with those requirements. QAO's annual reports are a useful source for obtaining information regarding our structure and business. The plan and annual reports can be accessed through our website www.qao.qld.gov.au.

2. Personal information

For all Information Privacy Principles other than IPPs 6 and 7, which refer to access and amendment provisions, personal information is defined in the information standard as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and 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".

The information does not have to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. The information could be held in paper or electronic records and is not limited to confidential or sensitive personal details.

Personal information for the purpose of IPPs 6 and 7 is limited to information concerning an individual's "personal affairs" as the phrase "personal affairs" has been interpreted in the *Freedom of Information Act 1992*.

QAO is committed to ensuring that all personal information held is managed with integrity and in accordance with the 11 IPPs.

2.1 Exemptions to non-disclosure of personal information

The IPPs do not apply to certain exempt bodies such as commissions of inquiry nor to personal information contained in documents concerning covert police activity, witness protection, disciplinary actions and misconduct, whistleblowers, Cabinet and Executive Council and commissions of inquiry.

It should be noted that compliance with the Information Standard is administratively based. This means that, where conflicting requirements exist, any legislative requirements will supersede compliance with the Standard. ie. personal information obtained as "protected information" by QAO under the *Financial Administration and Audit Act 1977*.

3. Acts that effect the Queensland Audit Office

There is a range of legislation that affects the way that QAO processes information, including personal information.

The most significant Act affecting the activities of QAO is the *Financial Administration and Audit Act 1977* (the Act). Section 92 of the Act prescribes the confidentiality provisions in regard to information obtained under this Act. Every person who is or has been an authorised auditor, as defined by the Act, or a person engaged or employed by a contract auditor, must not divulge or communicate information obtained or disclosed under or for the purposes of the Act except for purposes prescribed under the Act.

Section 92(3) of the Act does not however prevent disclosure of such information to:

- the Parliamentary Committee; or
- the Public Works Committee; or
- the Crime and Misconduct Commission; or
- a police officer, or a person or body responsible for the investigation or prosecution of offences, if the information relates to the investigation or prosecution of an offence; or
- a court for the purposes of the prosecution of a person for an offence.

Section 39 of the *Freedom of Information Act 1992* specifically exempts any audit matter from freedom of information disclosure if its disclosure is prohibited by section 92 of the *Financial Administration and Audit Act 1977* unless disclosure is required by a compelling reason in the public interest.

The legislative requirements of the *Financial Administration and Audit Act 1977* and the *Freedom of Information Act 1992* in relation to information obtained during the course of an audit will supersede compliance with *Information Standard 42 – Information Privacy*.

4. Types of personal information held by the Queensland Audit Office

QAO holds electronic and paper records containing personal information which can broadly be divided into personal information records relating to QAO employees including contractors, personal information obtained under the public sector auditing program and personal information relating to the service delivery functions of QAO.

Personal information held by QAO can be broadly classified under the following record categories:

- client related records
- contract auditor related records
- employee personnel records
- financial management system information
- information systems personal information
- Office of the Auditor-General and other QAO records
- alumni records.

4.1 Client records

In conducting our audits, QAO may collect personal information about persons associated with or employed by its clients or their business contacts.

QAO uses business contact details to assist in the provision of audit services and to raise awareness about professional developments that may be of relevance or interest to clients.

Executive and Personal Assistants and delegated staff may amend this information.

Personal information obtained in the performance of an audit may be kept on audit related hard copy and electronic files.

Such information is obtained by QAO under the legislation referred to in Section 3 and exempt from disclosure other than as prescribed by the legislation. Under the legislation certain personal information may be included in QAO published reports at the discretion of the Auditor-General.

Personal information held in audit work papers is normally retained for a minimum period of 7 years whilst any personal information on the audit report will be retained permanently. These retention periods have been approved by Queensland State Archives. Appropriate storage and security arrangements as detailed in our Information Security Policy will apply depending on the sensitivity of the information.

4.2 Contract auditor records

QAO collects personal information about individuals applying to be registered as contract auditors who can provide audit services to the Auditor-General.

Personal information provided on applications details employment history, work preferences, qualifications, experience, insurance and business contact details. This information is used to assess the suitability of applicants to be registered and eligible for audit appointments on the Contract Auditor database, as well as ensuring continuing awareness about professional developments and standards required in the conduct of audits undertaken on behalf of the Auditor-General. Personal information (names) may also be included in QAO published reports at the discretion of the Auditor-General.

These records are retained for a minimum period of 7 years as approved by Queensland State Archives however some personal information may be filed on the audit reports and as such be retained permanently. Appropriate storage and security arrangements as detailed in our Information Security Policy will apply depending on the sensitivity of the information.

Personal information is not disclosed to other persons or organisations, except as set out in Section 2 of this plan.

4.3 Employee personnel records

Employee personnel records include personnel and payroll, recruitment and other records. The purpose of these records is to maintain employment history and payroll and administrative information relating to all current and former permanent, contract and temporary staff members of QAO. The People and Performance section manages these records.

4.3.1 Personnel and payroll

The records may include any one or more of the following:

- records relating to attendance and overtime
- leave applications and approvals
- medical records
- payroll and pay related records, including banking details
- tax file number declaration forms
- declarations of pecuniary interests
- personal history files
- performance appraisals
- records relating to personal development and training
- trade, skill and aptitude test records
- completed questionnaires and personnel survey forms
- travel documentation
- records relating to personal welfare matters
- contracts and conditions of employment.

4.3.2 Recruitment

The records may include any one or more of the following:

- recruitment and selection records
- records relating to relocation of staff and removal of personal effects
- records relating to character checks, security clearances and criminal history.

4.3.3 Other records

The records may include any one or more of the following:

- records of accidents and injuries
- compensation case files
- rehabilitation case files
- records relating to counselling and discipline matters, including disciplinary, investigation and action files, legal action files, and any other staff and establishment records as appropriate
- complaints and grievances
- recommendations for honours and awards.

People and Performance staff, employee supervisors and the employee to whom a particular record relates have access to personnel records.

Personnel records are stored on paper and electronic media and are kept for variable periods according to the applicable provisions of the General Disposal and Retention Schedule for Administrative Records issued by Queensland State Archives. Appropriate storage and security arrangements as detailed in our Information Security Policy will apply depending on the sensitivity of the information.

Personal information held in personnel records may be disclosed outside QAO, as appropriate, to the Australian Taxation Office, QSuper, Public Service Commission, police, courts and third parties such as banks and insurance companies (name and account numbers only). Certain personal information (names and qualifications) may also be included in QAO published reports at the discretion of the Auditor-General.

4.4 Financial management system information

The purpose of these records is to process and account for the expenditure and revenue of QAO. General content may include name, address and service or goods category. Sensitive content may include financial information including debts. The personal information relates to creditors and debtors, including outsourced service providers if they are identified personally. Financial administration staff and staff within relevant business areas have direct access to this personal information.

The records are stored on paper and electronic media and are kept according to the categories set out in the General Disposal and Retention Schedule for Administrative Records issued by Queensland State Archives. Appropriate storage and security arrangements as detailed in our Information Security Policy will apply depending on the sensitivity of the information. Personal information is not disclosed to other persons or organisations, except as set out in Section 2 of this plan.

4.5 Information systems personal information

QAO's Information Technology (IT) systems routinely carry, enable processing of, and store, for varying periods, the core business transactions and the supporting corporate service business transactions. These transactions encompass both internal electronic transactions and external transactions, including telephone, e-mail, Internet, Extranet and government Intranet activity.

There are also personal information records relating to IT system administration, particularly system security identifiers and usage tracking records that are held by central IT administrators and managers. These records are stored on both paper and electronic media.

This information is only disclosed to managers, system administrators and the individual officers concerned. Appropriate storage and security arrangements as detailed in our Information Security Policy will apply depending on the sensitivity of the information. On accessing the network, staff are made aware of system usage rules and monitoring procedures concerning misuse of information.

4.6 Office of the Auditor-General and other QAO records

Inwards correspondence addressed to the Auditor-General or QAO staff from the public or other government agencies on a wide array of matters concerning official business or public concern and may result in the preparation of advice and responses. QAO keeps copies of the inwards and outwards documentation in electronic and paper form.

These records may include personal information, which might arise in any subject matter related to the Auditor-General's responsibilities. Examples include names, addresses, personal opinions about public administration matters, occupational and organisational information about persons, complaints and grievances subject matter, and any other matter that the correspondent wishes to convey about themselves or personally identifiable third parties in government or amongst the public.

QAO staff who have access to the Office of the Auditor-General and QAO correspondence records are on a "need to know basis". Any personal information is not disclosed to other persons or organisations, except as set out in Section 2 or as required by legislation.

Records of the Office of the Auditor-General and QAO containing personal information are subject to appropriate storage and security arrangements as detailed in our Information Security Policy depending on the sensitivity of the information. These records are retained for periods as approved or recommended under Retention and Disposal Schedules authorised by Queensland State Archives.

4.7 Alumni records

QAO holds, on behalf of the QAO Alumni Association Inc., personal information about individuals (ex-staff members) applying to become members of the association.

Personal information provided by individuals details names, contact details and financial information regarding fees and donations. This information is used by association members to record membership and to advise members of business, forthcoming functions and events of interest.

This personal information is not disclosed to other organisations or unauthorised staff of QAO and is held until administrative use ceases.

5. Existing contracts, licences and outsourcing arrangements

QAO has entered into contractual arrangements with a number of service providers for audit and administrative functions. These contracts are ongoing and in some cases span a number of years.

The majority of contracts are with audit service providers. These individuals are suitably qualified people, noted by QAO for consideration for audit appointments on behalf of the Auditor-General.

All new contracts include appropriate clauses covering privacy compliance issues.

6. Review schedule

Objective	Tasks
Assessment of Current Practices	Review types of information held, identify personal information held and ensure compliance with principles. Identify any areas of risk or exposure under applicable Information Privacy Principles and adopt appropriate procedures to mitigate risk.
Disclosure	Business units to ensure compliance with procedures regarding collection, use and storage of personal information.
Awareness	Continue awareness training to new staff and review privacy related information on the intranet. Clients and the public can access QAO's Privacy Plan on the Internet and copies are available on request.
Compliance	Periodic update of Privacy Plan and associated materials.

7. Procedure to access and amend personal information

Employees of QAO can access their personnel records and may request alteration of their personnel information through administrative process.

Requests from individuals wanting to update personal information, such as change of address, will be directed to officers responsible for the management of that information. The Privacy Contact Officer is the appropriate point of contact if there are issues concerning access to or amendment of personal information and the IPPs. The Privacy Contact Officer can advise on these matters and legislative requirements governing such access under the *Freedom of Information Act 1992* upon request.

Any applications about personal affairs (as defined by the *Freedom of Information Act 1992*) are free. Personal affairs are more matters of a private or personal nature such as health, medical, family relationships and financial obligations

The *Freedom of Information Act 1992* is available on the Office of the Queensland Parliamentary Counsel website at www.legislation.qld.gov.au.

8. Complaint and review procedures

If an individual believes that QAO has not dealt with their personal information in accordance with an Information Privacy Principle, they may make a complaint to QAO seeking an investigation. A complaint must be in writing and made within six months from the date when the breach was suspected to have occurred. As much relevant information as possible about the alleged breach of the IPPs should be provided.

Complaints should be forwarded to:

Privacy Contact Officer
Queensland Audit Office
GPO Box 1139
BRISBANE QLD 4001

Email requests will also be accepted to privacy.officer@qao.qld.gov.au. The Privacy Contact Officer can also be contacted on (07) 3405 1144 to provide more information about complaint handling procedures.

Complaints will be acknowledged in writing within 14 days of receipt of the complaint. The delegated decision-maker will consider all requests and QAO will process formal requests within 60 days from the date on which the complaint was received. Applicants will be advised in writing of QAO's decision.

If an applicant does not agree with QAO's decision, they can request an internal review. The Auditor-General 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 Auditor-General will provide a response in writing to the individual.

The postal address for internal review applications is:

The Auditor-General
Queensland Audit Office
GPO Box 1139
BRISBANE QLD 4001

Officers involved with any review will also be cognizant of procedures outlined in our Complaints Handling Policy.

9. Information Privacy Principles

The Information Privacy Principles set out in Information Standard No 42 cover collection, storage, use and disclosure of personal information. Many of the principles only require that "reasonable" steps be taken having regard to the circumstances. Factors which will determine the "reasonableness" of steps to be taken will include the sensitivity of the information, the possible uses of the information, the context in which it was obtained and the financial and practical effects of strategies for compliance on the continued ability of the business unit to perform its legitimate functions.

A summary of the Information Privacy Principles is set out in Appendix A.

Appendix A – Summary of information privacy principles

Queensland Government agencies must comply with the following 11 Information Privacy Principles:

- 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: Recordkeeper to check accuracy 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

The main points of each of the Information Privacy Principles are:

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

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
- (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
 - (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
 - 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
 - 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.

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 authorized 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
 - 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
 - (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.

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.

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
 - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

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
 - (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.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.
3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.