



# **Privacy Plan**

## **Department of Industrial Relations**

## TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	PERSONAL INFORMATION	3
3.	INFORMATION PRIVACY PRINCIPLES	4
4.	OBJECTIVES	4
5.	RESPONSIBILITIES	6
6.	LEGISLATIVE REQUIREMENTS THAT SUPERCEDE PRIVACY PRINCIPLES	6
7.	POLICIES RELATING TO PERSONAL INFORMATION	6
8.	ROLE OF THE DEPARTMENT\ACTS ADMINISTERED	7
9.	PERSONAL INFORMATION HELD\RETENTION PERIODS	7
10.	CONTRACTUAL ARRANGEMENTS	8
11.	ACCESS TO AND CORRECTION OF PERSONAL INFORMATION	8
12.	COMPLAINT AND REVIEW PROCEDURES	9
13.	IMPLEMENTATION OF THE PRIVACY REGIME IN DIR	10
	APPENDIX A – SUMMARY OF INFORMATION PRIVACY PRINCIPLES	12
	APPENDIX B – TYPES OF PERSONAL INFORMATION HELD BY THE DEPARTMENT OF INDUSTRIAL RELATIONS	18

## 1. INTRODUCTION

The Queensland public sector privacy scheme was introduced in September 2001 through Information Standard 42 (*IS42*). This Privacy Plan has been developed to ensure the Department's compliance with the information privacy principles set out in IS 42 and supporting Guidelines. This Standard will have the effect of introducing over time into the Queensland public sector, the information privacy principles contained in the Commonwealth Privacy Act 1988.

Compliance with IS 42 and the 11 Information Privacy Principles is administratively based. This means that where conflicting requirements exist, legislative requirements will prevail over compliance with the Information Standard.

The Information Standard and its relevant Guidelines require each "Queensland Government Agency" to prepare and publish a Privacy Plan approved by the relevant Chief Executive Officer by April 2002. The Department of Industrial Relations first published its Privacy Plan on 22 April 2002. This version has been developed as a result of subsequent reviews.

This plan is written in a way, which takes into account the diverse range of functions of the Department of Industrial Relations. It aims to provide: -

- guidance to members of the public to assist them to understand how personal information is managed in the Department and how they can exercise their privacy rights in respect of the Department's activities;
- guidance to officers in the Department who deal with personal information on the requirements of *IS42* and its guidelines;
- an implementation plan for achieving full compliance with those requirements; and
- identification of procedures/practices, which have been adopted by the Department to eliminate or reduce the risk of non-compliance.

## 2. PERSONAL INFORMATION

The purpose of *IS42* and its Guidelines is to establish a framework for the responsible collection and handling of personal information in the Queensland Government public sector. There is a summary of the [11 Information Privacy Principles \(IPPs\) in Appendix A](#) of this plan. Personal Information is defined in the Information Standard as being:-

*Personal Information for the purposes of all Information Privacy Principles other than Information Privacy Principles 6 and 7 means 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.*

Examples include an individual's name and address, telephone number, employment information, email address, birth date, drivers licence number, identifying characteristics such as birthmarks, tattoos, and psychological profiles. It also includes sensitive information such as political and religious beliefs, medical records, disabilities and sexual preferences.

*Personal Information for the purpose of Information Privacy Principles 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.*

Examples include individual's signatures, financial obligations, health or ill health, domestic responsibilities, affairs relating to family and marital relationships, and a person's income and personal financial position.

The information does not have to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. It is not limited to confidential or sensitive personal details. It covers information held in paper or electronic records or in any other medium such as audio, video or digital format.

In certain instances personal information is exempt under the provisions of *IS42*, such as:

- Disciplinary actions and misconduct matters;
- Whistleblowers;
- Cabinet and Executive Council documents; and
- Commissions of Inquiry.

### **3. INFORMATION PRIVACY PRINCIPLES**

The Queensland privacy regime is based on the Commonwealth Government Information Privacy Principles (IPP's) contained in the *Privacy Act* 1988. The information privacy principles are 11 general principles that set the privacy standards with which agencies must comply. The aim of the principles is to minimise the risk of misuse of personal information. They also allow individuals to exercise a reasonable degree of control over what happens to their personal information.

To these ends, the principles establish standards for:

- the collection;
- storage and accuracy;
- public awareness and subject access\alteration; and
- use and disclosure to third parties of personal information.

Staff of the Department must comply with the information privacy principles unless an exemption applies. A complete outline of the [information privacy principles is provided at Appendix A](#).

### **4. OBJECTIVES**

It is the objective of this Department to remain compliant with *IS42* to achieve the following outcomes with respect to personal information:

- We will only collect personal information that is relevant and necessary to what we do.
- We will not keep personal information we do not need unless we are legally required to do so. We may be required to keep records for standard periods of time for reasons relating to auditing, fraud prevention or other reasons.
- When we collect information, we will not;

- break the law,
  - mislead people, or
  - harass people.
- If we collect information from you about yourself, we will tell you;
  - how we will use that information,
  - why we are collecting the information, and
  - who else we may give the information to.
- We will only use or release personal information for activities which are directly related to the original reason we collected it, unless:
  - (a) it is required by law or needed for a criminal investigation;
  - (b) it will lessen a serious and imminent threat to a person's life or health;
  - (c) we believe an offence has been committed and we tell the relevant authorities;
  - (d) we have the permission of the person that the information concerns.
- We will protect the personal information we hold from misuse and loss and from being disclosed to or seen or changed by people who are not authorised by us.
- We will make available details on what personal information we hold and how we use that information.
- If you ask us, we will tell you what information we hold about you unless there are important public interest reasons not to, as detailed in the *Freedom of Information Act 1992* or other relevant legislation. This may happen if:
  - (e) we can not tell you without breaching someone else's privacy;
  - (f) we can not tell you without endangering an investigation or legal action; or
  - (g) there are other important reasons.
- We try to keep personal information accurate and up-to-date. Depending on the purpose of the information, we will endeavour to ensure that it is correct before relying on it.
- If you have access to a document, which contains information concerning your 'personal affairs' information (as described in the *Freedom of Information Act 1992*) that is inaccurate, incomplete, out-of-date or misleading, you can apply in writing to have the information amended or corrected.
- When other government or non-government bodies are involved in collecting, storing or using personal information for us, or have access to personal information that we hold, we will require them to meet this standard of privacy protection in that work.

## 5. RESPONSIBILITIES

Overall responsibility for privacy matters rests with the Director-General. The Department's privacy contact officer details are as follows:

Privacy Contact Officer - DIR  
 Administrative Law Unit  
 Executive and Strategic Services  
 Department of Industrial Relations

GPO Box 69  
Brisbane QLD 4000  
Ph: (07) 323 96783

## **6. LEGISLATIVE REQUIREMENTS THAT SUPERCEDE PRIVACY PRINCIPLES**

Legislation provisions that supersede the requirements of the privacy principles are found in the following:

- *Acts Interpretation Act 1954;*
- *Financial Administration and Audit Act 1977;*
- *Financial Management Standard 1977*
- *Freedom of Information Act 1992;*
- *Industrial Relations Act 1999;*
- *Public Records Act 2002;*
- *Public Service Act 1996;*
- *Workers' Compensation and Rehabilitation Act 2003;* and
- *Workplace Health and Safety Act 1995.*

The Department will continue to identify any other legislation that may impact on the principles.

## **7. POLICIES RELATING TO PERSONAL INFORMATION**

Issues of privacy and confidentiality are currently addressed in various policy documents that bind the Department. These documents include:

- The Code of Conduct;
- The Record Keeping Policy and Principles;
- Administrative Instruction No 20 – Records Management Practices;
- Information Standard 18 – Information Security;
- Information Standard 24 – Policies for the Management of Information within Government;
- Information Standard 31 – Retention and Disposal of Government Information;
- Information Standard 40 – Record keeping;
- Corporate Information Management Policy;
- Corporate Information Security Standard; and
- Workplace Health & Safety Queensland Administrative Release Policy.

## **8. ROLE OF THE DEPARTMENT\ACTS ADMINISTERED**

The Department's mission is to achieve productive, safe and fair jobs for Queenslanders. To achieve its goals, the Department may seek and hold personal information under the following legislation, which it administers:

- *Industrial Relations Act 1999;*
- *Trading (Allowable Hours) Act 1990;*
- *Public Service Act 1996;*

- *Anzac Day Act 1995*;
- *Private Employment Agents Act 1983*;
- *Holidays Act 1983*;
- *Pastoral Workers' Accommodation Act 1980*;
- *Workers' Accommodation Act 1952*;
- *Workplace Health and Safety Act 1995*;
- *Electricity Safety Act 2002*.

## 9. PERSONAL INFORMATION HELD\RETENTION PERIODS

To perform its functions, the Department holds a wide range of personal information in both electronic and paper records. The main classes of personal information held are provided in [Appendix B](#). The majority of corporate records are managed by our Shared Service Provider, Corporate Solutions Queensland on behalf of this Department.

The Department maintains two public registers i.e. registers of personal information required by law to be open to, or otherwise available for, public inspection whether or not on payment of a fee.

These are the **electrical contractors licence register** and the **electrical workers licence register** either of which may be viewed by the public at the Electrical Safety Office website at [www.eso.qld.gov.au](http://www.eso.qld.gov.au)

The *Public Records Act 2002* governs the making and preservation of public records in Queensland. Pursuant to this Act, Queensland State Archives has compiled a *General Disposal and Retention Schedule for Administrative Records*, which has been adopted by the Department as the template for setting retention and disposal times and methods. A copy of this schedule can be found at [http://www.archives.qld.gov.au/index\\_publications.html](http://www.archives.qld.gov.au/index_publications.html).

Managers must ensure that staff are aware of their responsibilities for the retention, storage and disposal of departmental records including personal information in accordance with the *Public Records Act 2002* and related schedules, the information privacy principles and the requirements of [Administrative Instruction 20 – Records Management Practices](#).

## 10. CONTRACTUAL ARRANGEMENTS

The Department regularly enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties or the collection of personal information by third parties on behalf of the Department.

Any contracts entered into prior to April 2002 may not comply with the principles. Upon renewal of existing contracts, and/or the establishment of new contracts that may involve the sharing/managing of personal information since this date, the department will include a privacy clause to ensure compliance with *IS42*.

## 11. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

The rights of individuals to access and correct personal affairs information held by the Department is principally governed by the provisions of the *Freedom of Information Act 1992(FOI Act)*.

*IS42* also provides controls on how *personal information* is managed. The rights of access and amendment are dealt with in Information Privacy Principles (IPPs) 6 and 7. Those rights are confined to the person to whom the personal information directly and personally relates.

**IPP 6 basically provides that a person is entitled to access any record that contains their *personal information* except where access is restricted by any law.**

**IPP 7 basically provides that a person is entitled to seek an amendment of any record that contains their *personal information*, which is misleading, irrelevant, not up-to-date or incomplete.**

However, *IS 42*, qualifies those access and amendment rights by saying that they are limited to existing rights under the *FOI Act*. This means that *personal information* for the purpose of IPPs 6 and 7 is limited to information concerning an individual's *personal affairs* as interpreted in the *FOI Act*.

In summary, access to, or amendment of, personal information records in the Department of Industrial Relations, is subject to the following:

- the IPPs limiting the access and amendment rights and processes to those provided in the *FOI Act*; and
- applications for documents or application for correction or amendment being processed under the *FOI Act* provisions.

Completed applications can be lodged in person or by post. The addresses are:

Manager – Administrative Law Unit  
Department of Industrial Relations  
Level 6 Block B  
Neville Bonner Building  
75 William Street  
Brisbane Qld 4000  
or

GPO Box 69  
BRISBANE QLD 4001

Phone: (07) 323 96783  
Facsimile: (07) 322 51454

An additional avenue for individuals to access their personal information exists via the department's Workplace Health & Safety Queensland and Electrical Safety Office Administrative Release Policy. Certain classes of records can be accessed this way. For more information please refer to the policy.

## **12. COMPLAINT AND REVIEW PROCEDURES**

If an individual considers that the Department has not dealt with their personal information in accordance with the privacy principles, he\she is entitled to lodge a complaint and request an investigation. The complaint must be in writing, outline the basis for the complaint and provide as much detail as possible.

The department has a Complaints Handling Procedure which can be located on the Intranet at <http://irnet/quality/dirp02.pdf> Written complaints should be sent to the:

Privacy Contact Officer  
Administrative Law Unit  
Executive and Strategic Services  
Department of Industrial Relations  
GPO Box 69  
Brisbane QLD 4000

Ph: (07) 323 96783  
Fax: (07) 322 51454  
Email: [privacycontactofficer@dir.qld.gov.au](mailto:privacycontactofficer@dir.qld.gov.au)

and lodged within 6 months from the date when the breach was suspected to have occurred.

Complaints will be acknowledged in writing within 14 days from the date that the application was received and shall be processed by the Department within 60 days. Applicants will be advised in writing of the outcome including any remedies considered necessary to resolve the complaint.

If an applicant does not agree with the Department's decision, they can apply in writing to the Internal Review Officer – Privacy, for internal review of the initial decision. Applications for internal review must be made within 28 days of the complainant receiving advice regarding the outcome of the initial investigation. The postal address for internal review applications is:

Internal Review Officer – Privacy  
Administrative Law Unit  
Executive and Strategic Services  
Department of Industrial Relations  
GPO Box 69  
BRISBANE QLD 4001

The internal review will be carried out by an officer who is no less senior than the initial decision-maker and who has not previously been involved with the matter. The officer will complete the internal review within 45 days of receipt of the application and will provide the applicant with a written response outlining the outcome of the review and any action taken.

The Privacy Contact Officer can provide more information about the department's complaint handling procedures.

### **13. IMPLEMENTATION OF THE PRIVACY REGIME IN DIR**

The Department of Industrial Relations (DIR) embarked on an implementation program in early 2003 that included the introduction of a departmental Privacy Plan, formal complaints procedure and the development and delivery of state wide training to employees.

The department has identified that informing staff of their privacy responsibilities plays a critical role in our maintaining compliance within the requirements of IS42 and related guidelines.

To ensure a general awareness of the issues and the principles involved, a number of general strategies for compliance with the IPPs have been identified for adoption by the Department as a whole and for adaptation where necessary by individual program areas. These strategies have been grouped together below under the IPPs' main areas of coverage.

**Collection** - all application forms used to collect personal information from clients or employees are being reviewed to ensure that notification requirements (as per IPP2) are met, and authorisation for further disclosures is covered where necessary to the operation of the program area. The Department's website includes the Privacy Plan and Statement and an Information Privacy site for further information. Pamphlets and brochures have been developed and will be provided to clients advising them of how their personal information will be managed within the Department.

**Storage** - The Department continues to review and develop policies for storage of electronic and paper information with reference to the Department's and whole of government policies. Electronic records/databases have been reviewed to include password protection where required.

**Use** - Where information is stored in a computerised database, programmers are ensuring that appropriate descriptions are used to avoid errors or misinterpretation of data and standards are adopted which allow consistent and accurate use of personal information. Current policies and practices with reference to the functions and purposes of the particular programme areas are constantly being reviewed and amended to ensure personal information is used only for the authorised purposes for which it was collected.

**Disclosure** – Executive and Strategic Services in collaboration with program areas will continue to assist with the development of procedures to cover the main kinds of personal information staff can be expected to disclose and the authority for such disclosures.

#### **Additional strategies –**

All staff will continue to have access to training in the application of IPPs and the requirements of *IS42* through presentations arranged via the Privacy Contact Officer or in house training provided by Managers/Supervisors using the Information Privacy Resource Kit. This kit is available within each Regional Office.

This privacy plan is an evolving document and is to be reviewed and updated at least annually.

## **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 IPP.

### **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; and
- 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:
  - (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
  - (b) the purpose for which each type of record is kept;
  - (c) the classes or types of individuals about whom records are kept;
  - (d) the period for which each type of record is kept;
  - (e) 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
  - (f) 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:
  - (a) is accurate; and
  - (b) 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.

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;
3. 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.
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; 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.
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.

## **APPENDIX B - PERSONAL INFORMATION DIGESTS**

### **GENERIC CORPORATE RECORDS**

There are several categories of corporate records containing personal information that relate to all units of the Department. They are:

- employee personnel records;
- financial management system information;
- information systems personal information;
- contact\mailing lists; and
- ministerial\director-general correspondence.

The central repositories and computer databases for many of these records are managed and maintained under a Memorandum of Understanding with Corporate Solutions Queensland.

Due to the commonality of these records, they have been grouped together using the following generic descriptions.

#### **Employee Personnel Records**

The purpose of these records is to maintain employment history and payroll and administrative information relating to all permanent, contract and temporary staff members and employees of an agency.

It should not be assumed that all records described are kept in a common storage facility. Separate security arrangements will typically apply, depending on the sensitivity of the information. Records may be located on the human resources computer database (AURION), in human resource management units, individual units of the Department and/or our Shared Service Provider, Corporate Solutions Queensland.

Current and former employees and other persons (for example, spouses and next of kin who believe that the department's personnel records may also contain personal information about them) can obtain details of specific record handling practices of particular units by contacting supervisors in those units. If the unit's name is not known, individuals may contact the Department's Manager - Administrative Law Unit for further guidance.

#### **Personnel and payroll**

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

- (1) records relating to attendance and overtime;
- (2) leave applications and approvals;
- (3) medical records;
- (4) payroll and pay related records, including banking details;
- (5) tax file number declaration forms;
- (6) declarations of pecuniary interests;
- (7) personal history files;
- (8) performance appraisals, etc;
- (9) records relating to personal development and training;
- (10) records relating to library usage;

- (11) trade, skill and aptitude test records;
- (12) completed questionnaires and personnel survey forms;
- (13) records relating to removals;
- (14) travel documentation;
- (15) records relating to personal health/welfare matters; and
- (16) contracts and conditions of employment.

## **Recruitment**

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

- (1) recruitment records;
- (2) records relating to relocation of staff and removals of personal effects; and
- (3) records relating to character checks and security clearances.

## **Other records**

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

- (1) records of accidents and injuries;
- (2) compensation case files;
- (3) rehabilitation case files;
- (4) records relating to counselling and discipline matters, including disciplinary, investigation and action files, legal action files, records of criminal convictions, and any other staff and establishment records as appropriate;
- (5) complaints and grievances; and
- (6) recommendations for honours and awards.

Contents of employee personnel records may include: name, address, date of birth, occupation, employee identification number, gender, qualifications, equal employment opportunity group designation, next of kin, details of pay and allowances, leave details, work reports, security clearance details and employment history. It may also include physical and mental health details, disabilities, racial or ethnic origin, disciplinary investigation and action, criminal convictions, adverse performance and security assessments, tax file numbers, relationship details and personal financial information.

Personal information on personnel records relates to current and former staff members and employees including contract and temporary staff. The following agency staff have access to personnel records: executive and senior personnel management staff, supervisors and members of selection committees (if appropriate), and the individual to whom the record relates.

Personnel records are kept for variable periods according to the applicable provisions of the Standard Retention and Disposal schedule for staff and establishment records issued by Queensland State Archives.

Information held in personnel records may be disclosed outside the Department, as appropriate, to:

- Australian Taxation Office
- Q-Super
- Office of Public Service Merit & Equity; and

- third parties such as Citec (for payroll processing including bank details and other personal deductions as authorised by employees).

Records relating to all current and former employees of the Department and may be stored on paper, microfiche and electronic media.

### **Financial Management Information System**

The purpose of these records is to process and account for expenditure and revenue.

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. The information may be found on the Department's financial accounting database (SAP), central accounting branches, individual units of the Department and/or our Shared Service Provider. Access to this personal information is restricted to the finance administration staff in the central accounting branch, the relevant unit of the Department and/or our Shared Service Provider.

The records are kept according to the categories set out in the standard Retention and Disposal Schedule issued by Queensland State Archives. Separate storage and security arrangements apply depending on which business area holds the records and the sensitivity of the information.

This information is not usually disclosed to other persons or organisations.

The records may be stored on paper and electronic media.

### **Information Systems Personal Information**

The Department's information management systems and data networks routinely carry, enable processing of, and store, for varying periods, much of the core business of the Department. It encompasses both internal electronic transactions and external transactions, including telephone, e-mail, Internet and government Intranet activity. This also includes information shared and managed within our Shared Service Provider.

The great bulk of those personal information records within that network environment are described above, or are described in the other parts of this plan that deal with the operations of service delivery arms of the Department. This extends to all individual and whole of agency e-mail address groups.

In addition to that material, there are some personal information records specifically tailored to IT system administration, namely IT system security identifiers and usage tracking records about staff users of the IT system that are held by central IT administrators and staff supervisors.

That information is not usually disclosed to persons other than staff supervisors, system administrators and the individual officers concerned. Staff are routinely made aware of system usage rules and monitoring procedures concerning collection and use of the information.

The records may be stored on paper and electronic media.

## **Contact/Mailing Lists**

Business units and staff from all areas of the Department maintain contact lists to enable fast and convenient retrieval of contact details relating to:

- other Departmental or State Government staff;
- clients or stakeholders of the Department;
- suppliers and service providers.

The contact lists may include personal information on individuals such as name, address (postal and e-mail), telephone or fax numbers (as provided upon consent by an individual) and are used to communicate and/or consult with and/or provide data or information (electronic and hard copy) to the individual concerned.

This information may be freely available (eg telephone books) and may be stored electronically or in paper form. The information is not disclosed to third parties and is retained or destroyed in accordance with the State Archives Retention and Disposal Schedule.

## **Ministerial\Director-General Correspondence**

Inwards correspondence addressed to the Minister, the Director-General or their staff on matters of official business may be referred to the Department for consideration and preparation of advice and responses including outward correspondence. This correspondence may be found in the Minister's Office, the Director-General's office or relevant business units of the Department.

The Departmental staff who have access to these correspondence records are executive and senior officers, administrative staff who process the correspondence and departmental officers on a "need to know basis". The information is not usually disclosed to other persons or organisations.

The records under the control of the Department containing the personal information are retained for periods provided under the standard Retention and Disposal Schedule authorised by State Archives.

The Department keeps copies of the inwards and outwards documentation in electronic and/or paper form. These records may be held in the Minister's or Director-General's offices or the units responsible for preparing the responses. Those records include any personal information, which is likely to arise in any subject matter related to portfolio responsibilities. Examples might 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.

The Department of Innovation and Information Economy is developing a protocol for the disclosure of personal information by way of ministerial correspondence. This protocol will take into account any guidelines developed relating to disclosure for the purpose of informing the Minister or the Premier.

## **SERVICE DELIVERY RECORDS**

## **Managed By Corporate Solutions Queensland**

Our shared service provider, Corporate Solutions Queensland (CSQ) has been contracted to provide corporate and support services that enhance the service capabilities of the Department of Industrial Relations' delivery units. The services provided by CSQ relate mainly to the corporate information outlined above with a significant share of these records controlled by CSQ business units. These functions may include:

- acquisition, accounting and payroll services;
- asset and building services;
- financial management;
- information and business improvement services;
- information solutions;
- internal audit;
- legal and risk management;
- organisational learning; and
- workforce management.

---

## **Electrical Safety Office**

The Electrical Safety Office (ESO) is responsible for ensuring compliance by electricity entities and electrical contractors, workers, manufacturers and suppliers with the electrical safety and licensing legislation provisions of the Electrical Safety Act 2002. The Office also provides a range of regulatory, advisory and support services to the electrical industry and the general community.

ESO functions requiring the collection of personal information include the licensing of electrical workers and contractors and the investigation of suspected electrical fires and electrical incidents, electrical accidents (fatal and non-fatal) and complaints of unsatisfactory or unsafe electrical work.

Individuals about whom personal information is held include electrical workers and contractors as well as members of the public affected by electrical fires, incidents or accidents.

Personal information collected with respect to members of the public might include name, address, sex, age, contact details (phone, fax or email) and details of complaints made or information provided. Personal information collected regarding electrical workers and contractors might include name, contact details, date of birth, work and training history, insurance details, electrical licensing information, asset details, work standards and disciplinary actions.

Access to this information is generally available to senior executive and investigations officers of the ESO, members of the Electrical Licensing Committee and relevant ESO administrative officers. Some of the information collected is disclosed to other units in the Department and other government agencies. Retention and/or disposal of records containing personal information is carried out in accordance with the State Archives Retention and Disposal Schedule.

Access to the electrical contractors licence register and the electrical workers licence register is available to the public and may be viewed at the Electrical Safety Office website at [www.eso.qld.gov.au](http://www.eso.qld.gov.au)

---

## **Private Sector Industrial Relations**

The Division of Private Sector Industrial Relations collects personal information in order to conduct general (wages and conditions) inspections of workplaces, investigate complaints and disputes involving employers and employees, recover monies owing to employees and institute legal proceedings if necessary. The Division also collects personal information in the administration of the Anzac Day Trust, the granting of local public holidays and legislation administered by the industrial inspectorate.

An individual about whom personal information is held includes employers, employees, ex-service organisation representatives and heads of local government or community councils.

Personal information collected includes the name, address and contact details of employers and employees as well as employment information relating to the complaint or dispute. Personal information pertaining to the Anzac Day Trust and gazettal of public holidays is limited to the name and address of an office bearer in the responsible organisation.

The personal information is accessible only by investigating officers and administrative staff responsible for the activity. The electronic wage complaint system is protected by password entry.

In some instances, the personal information collected may fall under Federal legislation and, where appropriate, such information will be held in accordance with the IPP's as outlined in the *Privacy Act 1988*.

The personal information collected is not disclosed to third parties except for certain information relating to wage complaints.

Records containing the personal information are retained and/or disposed of in accordance with the State Archives Retention and Disposal Schedule.

---

## **Public Sector Industrial and Employee Relations**

The Division of Public Sector Industrial and Employee Relations perform a number of functions to assist agencies and Government with industrial and employee relations issues. Services include research, policy advice and development, advice on employment issues, advocacy or representation and employee training.

Due to their nature, most of the functions performed by the Division do not require the collection of personal information. The exception is the Public Sector Management Program (PSM Program) hosted by the Division. This program provides management education and training for middle and senior public sector managers. The PSM Program office manages the administration, assessment and accreditation of the program.

Personal information collected includes name, address, contact details, educational qualifications and employment history and may be shared with facilitators. Information regarding disabilities and diet is also collected and may be provided to training venues to assist participants.

Other than the facilitators and the venues, the information collected is not disclosed to third parties nor used for purposes other than that for which it was collected unless prior consent has been obtained. Access to the information is restricted to senior officers and staff directly involved in administering the activity.

Paper records are kept for 7 years and then destroyed. Electronic data is kept indefinitely.

---

## **Workplace Health and Safety Queensland**

The Division of Workplace Health and Safety Queensland (WHSQ) are responsible for developing workplace health and safety standards and enforcing those standards. To meet these responsibilities, WHSQ provides a number of services including the development of safety guidelines and regulations, the provision of advice or workshops for employers, employees and safety officers, the carrying out of workplace inspections, investigations or audits and the accreditation of workplace health and safety officer training providers.

The personal information collected in providing these services includes information relating to:

- accredited providers for Workplace Health & Safety Officers (WHSO) & Prescribed Occupations and all applicants who hold WHSO & Prescribed Occupations certificates. The information collected includes first name, middle name, surname, date of birth, residential address, mailing address, contact phone numbers and e-mail address.
- construction workplaces throughout Queensland where the project cost is greater than \$80000. The information includes the name of the payer, principal contractor, project location address of the site, type of project being undertaken, the estimated project value, project contact, contact telephone, project owner, owners address, phone number and fax number.
- appointments, inspections, investigations & audits including name, address, contact details of employers or employees as well as information relating to the subject of the visit. Personal information collected may be used in the issuing of infringement notices, improvement & prohibition notices, issuing of summons.
- ABR data is used strictly in accordance with Memorandum of Understanding and Service Level Agreements used in the Australian Taxation Office.
- designated doctors' list and health surveillance reports (Lead). Information includes doctors' names and addresses as well as names and a summary of health surveillance information relating to employee lead blood levels.

Records containing the personal information are kept in both electronic and paper mediums. Access to the bulk of this information is available to senior staff, investigating officers and administrative staff of the Division. Personal information is retained\disposed of in accordance with the State Archives Retention and Disposal Schedule.

---

## **Freedom of Information**

Personal information is collected when the Department receives a Freedom of Information request or a request to amend personal information under the *Freedom of Information Act*

1992 (*FOI Act*) from an individual. Some of the documents gathered to process the request may contain personal information (“personal affairs” as phrased under the *FOI Act*).

Staff in the Administrative Law Unit, Executive and Strategic Services, have access to this personal information. The recording of applicant personal details is maintained electronically and data can only be accessed by password.

The records are kept according to the categories set out in the Standard Retention and Disposal Schedule issued by Queensland State Archives.

This information is given to the Information Commissioner if the applicant and/or a third party requests an external review of the FOI decision. This information is not usually disclosed to any other persons or organisations.