



# Privacy Management Plan

## **1. Introduction**

**1.1.** This Privacy Management Plan is a plan for the Tribunal's compliance with the principles and requirements of the *Privacy and Personal Information Protection Act 1998* (the Act). The Act requires each "public sector agency" to prepare and implement a Privacy Management Plan.

**1.2.** It aims to give officers in Tribunal cost centres dealing with personal information guidance on the requirements of the Act, strategies for compliance with those requirements and to set down some procedures which can be adopted by the Tribunal to eliminate or reduce the risk of non compliance.

## **2. Personal Information**

**2.1.** The Act is concerned with "personal information". This is defined in the Act as being "any information or opinion about a person whose identity is apparent or can be reasonably 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. It is not limited to confidential or sensitive personal details. It covers information held in paper or electronic records and may even extend to body samples or biometric data.

**2.2.** While the definition of "personal information" is very broad, there are some important exceptions to the definition. The exceptions which are most relevant to the Department are:

- Information arising out of a Royal Commission or Special Commission of Inquiry;
- Information contained in Cabinet documents;
- Information about individuals who have been dead for more than 30 years;
- Information about an individual's suitability for appointment or employment as a public sector official;
- Information arising from the exercise of specific statutory law enforcement powers such as telephone interception, controlled operations and witness protection;
- Information contained in a publicly available publication;
- The exercise of judicial functions by a court or tribunal.

**2.3.** These exceptions do not interfere with the confidentiality or sensitivity of these types of information and exemption from the requirements of the Act does not mean that other policy or statutory requirements, such as the confidentiality of Cabinet documents, should be disregarded.

## **3. Main Classes of information collected, held and disseminated by the Tribunal**

**3.1.** Given the primary judicial function of the Tribunal, the range of holdings of non-exempt personal information is limited.

**3.2.** The Tribunal holds a range of information, some of which includes information which falls within the definition of "personal information" under the Privacy and Personal Information Protection Act. The main classes of such information held by the Tribunal and some pertinent matters affecting the way that information should be handled are:

### **3.3. Personnel records including:**

- Medical assessment records;
- Attendance and leave records;
- Recruitment, appeals, promotion and transfer records;
- Personal employee files and service records;
- Staff registers;
- Counselling and discipline records;
- Performance management and evaluation records;
- Training and apprenticeship records;
- Notices of separation and exit questionnaires;
- Occupational health and safety and workers compensation records; and
- Records of race, sex, marital status and impairments of employees for equal employment opportunity purposes

Personnel records may be held by the Tribunal's administrative services section or by individual cost centres. The Public Sector Personnel Handbook gives detailed directions on handling employee records in accordance with the Act and other relevant legislation.

Retention and disposal periods for specific classes of employee records are set out in the State Records Authority's Disposal Schedule - Personnel Records, March 1992.

Records of race, sex, marital status and impairments of employees for equal employment opportunity purposes are used only with the consent of the employees concerned for the identification of relevant opportunities or otherwise disclosed only in statistical form.

### **3.4. Administrative records including:**

- Vehicle usage;
- Telephone records from particular extensions;
- Network and electronic mail accounts;
- Stored electronic mail messages;
- Internet access and usage; and
- Records of public access to the Tribunal Web site

A large number of administrative records can contain personal information. Most of this information is collected automatically as a result of people using a particular service, eg, vehicles, telephone, e-mail, without any effort being made to identify individuals. The information becomes personal information by virtue of its potential, when accumulated, to create a profile of the activity or conduct of a particular officer or user of the services.

The identification of these kinds of records as containing personal information does not mean that the information cannot be used for the purposes for which it was collected. For example, the reasonable monitoring of telephone and Internet usage in accordance with Government policy would not be prevented. However, staff and website users should be made aware of how and why the information is collected and steps should be taken to ensure that the information is only used for the purposes for which it was collected or a directly related purpose.

### **3.5. Correspondence and Complaint files**

By reason of its judicial functions the Tribunal may have the benefit of exemptions from some Information Protection Principles when dealing with matters referred to it by an investigative agency or which could be referred to an investigative agency, such as the Home Building Service or Motor Vehicle Repair Industry Authority.

The Tribunal has in place standard complaints handling procedures which are consistent with relevant statutory requirements, the balancing of confidentiality against the right to adequate particulars of the complaint and the separation of active and inactive or closed complaint files.

Ministerial correspondence attracts an exemption from the Information Protection Principles relating to disclosure where personal information is disclosed by one agency to another agency under the administration of the same Minister for the purpose of informing the Minister or disclosure by an agency to an agency under the administration of the Premier for the purpose of informing the Premier.

### **3.6. Case files**

The Tribunal maintains a separate file for each case. To the extent that the information on each file relates to the exercise of judicial functions, it is exempt from the operation of the Information Protection Principles. However, this exemption does not apply to the administrative functions of the court or tribunal, particularly once the legal action has been finalised. In addition, records of Tribunal matters may be subject to suppression orders.

### **3.7. Transcripts and court and tribunal records**

The Tribunal maintains taped transcripts of all hearings heard at Tribunal managed venues. Transcripts are made for the benefit of the Tribunal, the parties to the action and other people and organisations with a legitimate interest in the case. Personal information in transcripts may also be covered by suppression orders or non disclosure orders, which can be enforced to prevent access by non parties.

## **4. Information Protection Principles**

**4.1.** The protections provided by the Act are based on 12 Information Protection Principles set out in the Act. They 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 Tribunal to perform its legitimate functions.

**4.2.** The Act also contains a number of exceptions to the operation of the principles. A summary of the Information Protection Principles together with a summary of the exceptions to the principles which are relevant to the Tribunal is set out at **Appendix A**. Tribunal officers are alerted to the need to consult the full text of the principles as they appear in the Act or in the Privacy NSW publication "A Guide to the Information Protection Principles". A copy of that publication has been provided to each cost centre in the Tribunal.

## **5. Privacy Codes of Practice**

**5.1.** Privacy Codes of Practice as provided for in the Act are statements of how a public sector agency proposes to depart from the Information Protection Principles or public register provisions of the Act.

**5.2.** As the overwhelming majority of the Tribunal's work is in relation to the hearing and determination of applications for orders, and is therefore exempt from the Information Protection Principles, there are no plans for the establishment of a Code of Practice. However, cost centre managers are directed to monitor their cost centre's capacity to comply with the principles and to alert senior management to any possible need for a Code of Practice.

## **6 Current Policies and Law Relating to Information**

### **6.1. What information must be provided in an application to the Tribunal?**

- An application made to the Tribunal must contain the following particulars:
- The name and address of the applicant;
- The name and last known address of each other party;
- A description of the order or orders sought by the applicant;
- A concise statement outlining the particulars of the dispute;
- The amount of money claimed in the dispute, if any;
- If applicable, the address of the premises to which the dispute relates; and If the applicant is a corporation – its ACN.

In addition, some applications must be made on a prescribed form. For example, as stipulated under the *Holiday Parks (Long Term Casual Occupation) Act 2002*.

This information is collected for a lawful purpose that is directly related to the primary function of the Tribunal to resolve disputes between parties. Failure to provide these details may result in the application being dismissed.

The provision of any additional information is voluntary.

### **6.2. What happens to the information on an application form to the Tribunal?**

The Registrar sends a copy of the application and any documents to the other person or persons in the dispute. In doing so, the Registrar observes all aspects of procedural fairness. Persons applying to the Tribunal should not include any confidential information they do not want disclosed to the other party or parties. The Registrar may consent to the withholding of the applicant's address from the application form only. This request, with reasons, must be made in writing with the application.

Any person may apply to the Registrar for access to records of proceedings in the Tribunal. While the Registrar must grant access, free of charge, to records of proceedings to any person who is a party to the proceedings, the Registrar also may grant this access to any other person who, in the opinion of the Registrar, has a sufficient reason for being given access to the record.

If a party does not want a document attached to an application file disclosed to a person other than a party to this application, the party must request that the Tribunal order that the document not be disclosed without the consent of the Tribunal.

### **6.3. Privacy and resolution of disputes before the Tribunal**

The Tribunal must initially endeavour to resolve any disputes through alternative dispute resolution methods such as conciliation or mediation. Any information discussed in these sessions is not admissible at any hearing or other legal proceedings.

If the dispute is not resolved through alternative dispute resolution it may be determined at a hearing. Hearings are conducted in public and are freely accessible to anyone.

However, if the Tribunal is of the view that the evidence or matters in the dispute are of a confidential nature the Tribunal may:

- Conduct the hearing wholly or partly in private;
- Prohibit or restrict the publication of the names and addresses of witnesses appearing before the Tribunal; and
- Prohibit or restrict the disclosure and publication of evidence before the Tribunal.

#### **6.4. Relationship between the Commissioner of Fair Trading and the Tribunal**

The Commissioner may request the Tribunal to provide information, which relates to any investigation or disciplinary action conducted by the Commissioner. The Tribunal must comply with any such request unless the Chairperson is of the opinion that to do so would compromise proceedings of the Tribunal.

The Chairperson may, if requested by the Commissioner, make available to the Office of Fair Trading any other information that is within the knowledge or possession of the Tribunal.

The Chairperson may also provide reports to the Minister or to the Commissioner concerning any matter the Chairperson considers:

- to be of importance in relation to the administration of the *CTTT Act 2001* or in relation to the jurisdiction of the Tribunal; or
- to be in the public interest.

#### **6.5. Information sought by the Tribunal**

The Tribunal can seek information from other government agencies. This information is required for the successful performance of its functions. The information includes:

- Business name details;
- Corporation details;
- Rental Bond Board information;
- Motor Vehicle dispute reports; and
- Building and Motor Dealer licensing details.

#### **6.6. Protection against improper disclosure of information**

A person performing lawfully authorised duties for the Tribunal must not disclose information obtained during the exercise of these duties, unless the disclosure is made:

- With the consent of the person to whom the information relates; or
- In connection with the operation of the *CTTT Act 2001*; or
- For the purpose of any legal proceedings arising out of the *CTTT Act 2001* or any report of such proceedings; or
- With any other legal excuse.

The penalty for any improper disclosure of information in contravention of the above criteria is a maximum of 50 penalty units or imprisonment for 12 months, or both.

#### **6.7. Storage of Personal Information**

Personal information held by the Tribunal is kept no longer than necessary, disposed of appropriately, protected by reasonable security safeguards, and protected from unauthorised use and/or disclosure.

Currently the maximum period for storage of Tribunal records is 10 years from the last action on the particular record.

#### **6.8. Who can access records of the Tribunal?**

Any person may apply in writing to the Registrar for access to records of proceedings in the Tribunal.

The Registrar must grant access, free of charge, to records of proceedings to any person who is a party to the proceedings.

The Registrar may grant access to a record of proceedings to any person who, in the opinion of the Registrar, has sufficient reason for being given access to the record.

However the Registrar will not provide access or copies of the following:

- Any note made by a Tribunal member, which was made for the member's own use and not intended to be part of the record of proceedings;
- Any documents which it has ordered not to be disclosed without its consent; and
- Any documents which it is prohibited to disclose by statute.

#### **6.9. What fees apply for copies of Tribunal records?**

The fee payable for a copy of a record of proceedings or any other document kept by the Tribunal is:

- \$2 per page or \$21 (whichever is greater) in the case of a written record or document; or
- \$21 per tape in the case of a sound or audio-visual recording.

A person who is or was a party to any proceedings is, however, entitled to a single free copy of any order made by the Tribunal in respect of the proceedings and of any written reasons given by the Tribunal in relation to that order.

The above fees may be waived (either in whole or in part) by the Registrar if the Registrar is satisfied:

- That the person required to pay it would suffer hardship if required to pay the fee; or
- It would be otherwise unfair or unreasonable for the person to have to pay the fee.

A separate schedule of fees applies to Strata Management Scheme dispute files.

#### **6.10. Publishing written decisions**

If a decision includes written reasons for the decision, the Tribunal may publish it on the Internet (<http://www.austlii.edu.au/au/cases/nsw/NSWCTTT/>). If any person searches the Internet using a person's name recorded in the decision, he or she may find the decision.

Prior to publication, decisions are examined, and if necessary altered, to protect the privacy of the individuals involved. This means that personal information such as the individuals' first names and street addresses will not be published.

#### **6.11. Other Legislation and Policies**

A range of other legislation affects the way the Tribunal processes personal information. In many cases such legislation prohibits disclosure of certain kinds of information except in specified circumstances. On the other hand, some legislation authorises the collection of information in a particular way or the sharing of information with other agencies. A list of such legislation appears at Appendix B. The most wide reaching and comprehensive legislation of this type is the Freedom of Information Act. The Privacy and Personal Information Protection Act makes it clear, however, that it is not intended to affect the operation of the Freedom of Information Act. There is also a range of Tribunal and whole of government policies which affect the way in which personal information is dealt with by cost centres. A list of such policies is at Appendix C.

## **7 Other considerations**

**7.1.** A number of other considerations, apart from expressed policy and statutory requirements, play a role in the way cost centres deal with personal information. It should be remembered by cost centres that compliance with or exemption from the requirements in the Act will not affect obligations arising under other legislation or under general law principles. Some matters for cost centres to continue to consider are obligations arising under principles of confidentiality, legal professional privilege, privilege for confidential professional communications and public interest immunity.

## **8 Public Registers**

**8.1.** Public Registers are defined in the Act as registers containing personal information that are made publicly available or open to public inspection. The Tribunal has no public registers, so defined.

**8.2.** It should be remembered that registers which do not fall within the public register requirements of the Act are still subject to the privacy information principles in the Act.

## **9 Internal and External Review Processes**

**9.1.** People who have complaints about how the Tribunal has dealt with personal information may apply to the Tribunal for "internal review". Applications for internal review may concern conduct by a cost centre which a person believes:

- breaches an information protection principle;
- breaches a code that applies to the Tribunal or one of its cost centres; or
- is an inappropriate disclosure by the Tribunal or one of its cost centres of personal information kept in a public register.

**9.2.** The Act sets out a number of requirements for the processing of applications for review including time frames, reporting requirements and requirements for advice to people about their rights to internal and external review.

**9.3.** The Tribunal has developed a procedure for the conduct of internal reviews. A copy of the procedure, which also canvasses external review by the Administrative Decisions Tribunal, is attached at [Appendix D](#).

## **10 Dissemination of Policies and Training**

**10.1.** The Tribunal offers training for staff which provide opportunities for disseminating policies and practices relating to the Tribunal's privacy obligations. All new staff complete a two day induction course including workplace ethics and privacy obligations. Relevant policies and practices are canvassed in this context.

**10.2.** The Office of Fair Trading's Code of Conduct, issued to all staff, deals with the use and disclosure of information obtained in the course of employment and with the confidentiality obligations of staff who have left the Department.

**10.3.** All staff have a copy of, or access to, this Privacy Management Plan. Information sessions are to be held on the Plan in each cost centre.

**10.4.** Training for staff is also supplemented by resources to be accessed when more complex decisions or assessments have to be made. Currently available resources include:

- Department circulars;
- Department guidelines and other publications including the Code of Conduct, Policy on Electronic Messages as Records, Records Management Policy, Standard on Full and Accurate Records, Policy On Electronic Record keeping and Standard on Records Management Programs;
- Publications from the Privacy Commissioner's Office, including:
  - the Guide to the Privacy and Personal Information Protection Act;
  - the Guide to the Information Protection Principles;
  - the Guide to Making Privacy Codes of Practice;
  - the Guide to Public Registers

## **11 External Service Providers**

**11.1.** The Tribunal has contractual arrangements with a range of service providers. These contracts are ongoing and in some cases span a number of years. Some were in existence prior to the commencement of the Act.

**11.2.** Existing contracts are being reviewed and updated to reflect the obligations of the Tribunal under the Act. New contracts will include appropriate clauses covering compliance issues.

## **12 Strategies for Compliance**

### **12.1. Assessment of Current Practices**

**12.1.1.** The first step in compliance with the Act and its principles is to assess current practice and procedure. The Tribunal can do this by:

- determining which types of information are held, by reference to Appendix B, and identifying the personal information contained in those holdings;
- determining the functions and purposes of the Tribunal by reference to relevant functions and the Business Plan;
- ascertaining the coverage of the Information Protection Principles and relevant exceptions to the personal information held, initially by reference to Appendix C and paragraph 2.2 above;
- referring to the current law and policies which already govern the way in which information is processed and ascertaining the policies and procedures adopted in compliance with those laws and policies; and
- identifying any remaining areas of risk or exposure under applicable Information Protection Principles.

**12.1.2.** If such areas of risk or exposure are identified then procedures must be adopted in line with or beyond the following general strategies for compliance. If the need for a Privacy Code of Practice is identified, this must be brought to the attention of Senior Management immediately (see paragraph 5 above).

**12.1.3.** A number of general strategies for compliance with the Information Protection Principles have been identified for adoption by the Tribunal as a whole and for adaptation where necessary by individual cost centres. These strategies have been grouped together below under the Information Protection Principles' main areas of coverage.

### **12.2. Collection**

**12.2.1.** For functions not subject to exemption from compliance with the Information Protection Principles, the Tribunal will review all application forms used to collect personal information from clients or employees to ensure that notification requirements (as per Principle 3) are met and consent to further disclosures is covered where necessary to the operation of the cost centre. The CTTT Web site will be similarly posted. Where necessary, interim pamphlets and/or stickers for this purpose will be provided to clients.

**12.2.2.** All Tribunal staff will be notified of programs and policies for monitoring of telephone, e-mail and internet usage.

**12.2.3.** Tribunal staff collecting personal information by telephone will be equipped with a form of words to notify clients of matters required by Principle 3 and to obtain consent to further disclosure where necessary. Alternatively, pro forma letters, confirming notification and consent will be forwarded to clients following telephone contact. In addition, where

telephone conversations are monitored by recording for quality control and supervision purposes, clients will be advised of this at the outset of the conversation.

### **12.3. Storage**

**12.3.1.** The Tribunal will further develop and review separate policies for storage of electronic and paper information with reference to the Office of Fair Trading's Records Management Policy and the Government's Security of Electronic Information Policy.

### **12.4. Use**

**12.4.1.** Where information is stored in a computerised database, the Tribunal will ensure that appropriate descriptions are used to avoid errors or misinterpretation of data and standards are adopted which allow consistent transfer of information between Registries and officers within the Tribunal.

**12.4.2.** Standards will be adopted, with reference to the functions and purposes of the Tribunal, to ensure personal information is used only for the purposes for which it was collected.

### **12.5. Disclosure**

**12.5.1.** The Tribunal will develop written procedures to cover the main kinds of personal information staff can be expected to disclose and the authority for such disclosures. Staff will be given additional training in the application of the Information Protection Principles to disclosure in the context of the Tribunal's functions.

**12.5.2.** Information disclosed by the Tribunal for research purposes will be anonymised.

**12.5.3.** The Information and Education Team of the Tribunal will, in consultation with the Minister for Fair Trading's Office and the Office of Fair Trading, develop a protocol for the disclosure of personal information by way of Ministerial correspondence. This protocol will take into account the exception contained in section 28(3) of the Act relating to disclosure for the purpose of informing the Minister or the Premier.

### **12.6. Internal Review**

**12.6.1.** Tribunal staff will be made aware through training and Tribunal circulars of the legal rights people have to internal review, and, in particular, what constitutes an internal review and the time limits for processing of internal reviews.

**12.6.2.** An internal review officer will be appointed and equipped by training and access to advice from the Privacy Commissioner's Office to deal with issues arising in any complaint. The internal review officer will be responsible for notifying the Privacy Commissioner.

**12.6.3.** An officer in the Information and Education Team of the Tribunal will be designated to be notified of each application for internal review to compile statistics on internal review for the Tribunal's Annual Report.

**12.6.4.** Individuals will be told about their rights to internal and external review through the inclusion of statements about these rights on forms and notices completed by people providing personal information. The format of such statements will take into account the exemptions from the Information Protection Principles afforded by the Tribunal's largely judicial function. However the statement will contain advice that:

- in relation to administrative functions, people have the right of access to, and correction of personal information about them;
- if they consider that personal information about them is being handled incorrectly, then they may request the Tribunal to undertake an internal review or they may contact the Office of the Privacy Commissioner;
- time limits apply to the making of applications, complaints and to the handling of internal reviews

**12.6.5.** Application forms for internal review will be provided to people wishing to apply for internal review. The application form will contain advice about:

- the range of action that may be taken by the Tribunal at the conclusion of the review;
- the time limits on the review; and
- the right of appeal to the Administrative Decisions Tribunal

## **12.7. Public Registers**

**12.7.1.** Any Tribunal public registers of information that may be created will be analysed in relation to the public register provisions of the Act and, to the extent to which those provisions apply to those registers, will adopt strategies for compliance with the Act's requirements.

# Privacy - Appendix A

## SUMMARY OF INFORMATION PRIVACY PRINCIPLES AND RELEVANT EXCEPTIONS

### Collection

1. Personal information should be collected lawfully and only when reasonably necessary for the purposes of the agency.
2. Personal information should be collected directly from the person to whom it relates unless that person has authorised collection from someone else or the person is under the age of 16 and the information has been collected from the person's parent or guardian.

#### Exceptions to Principle 2:

- law enforcement and investigative agencies where compliance might interfere with law enforcement or investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- any agency in connection with proceedings before a court or tribunal.

3. When personal information is collected reasonable steps must be taken to ensure that the person to whom it relates is aware:

- that the information is being collected;
- of the purposes of collection;
- of who will receive the information;
- of whether supply of the information is voluntary and the consequences of a failure to supply the information;
- of the person's right to access or change the information; and
- of the name and address of the agency collecting and holding the information.

#### Exceptions to Principle 3:

- any agency if collected for law enforcement purposes;
- an investigative agency where compliance might interfere with investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- where an agency is authorised or required not to comply under any Act or law;
- where compliance would prejudice the interests of the individual to whom the information relates;
- where the individual expressly consents.

### Storage

4. When personal information has been collected, the agency must take reasonable steps to ensure that the information is relevant to the purpose for which it was collected, not excessive, accurate, up to date, and complete and does not intrude to an unreasonable extent on the personal affairs of the person to whom it relates.

5. When personal information is held by an agency, it must ensure that the information is:  
kept no longer than is necessary for the purposes for which it is collected;  
disposed of securely when no longer needed;  
protected against loss and unauthorised use or dissemination by reasonable security safeguards; and  
similarly protected if, of necessity, transferred to a person in connection with the provision of a service to the agency, eg, a contractor or consultant.

Exception to Principle 5:

- investigative agencies

6. When personal information is held by an agency, it must take reasonable steps to enable any person to ascertain:

- whether the agency holds personal information in relation to the person; and
- the nature, main purposes of holding and how the person may gain access to the information.
- 

Exception to Principle 6:

- where an agency is authorised or required not to comply under any Act or law

7. When an agency holds information about a person it must, on request of the person, provide the person with access to the information without excessive delay or expense.

Exception to principle 7:

- where an agency is authorised or required not to comply under any Act or law

8. When an agency holds information about a person it must, at the request of the person, make appropriate amendments to ensure the information is accurate, up to date, relevant, complete and not misleading.

Exception to Principle 8:

- where an agency is authorised or required not to comply under any Act or law

## **Use**

9. An agency must not use personal information held by it without taking reasonable steps to ensure that the information is relevant, accurate, up to date, complete and not misleading.

10. An agency must not use personal information other than for the purpose for which it was collected unless:

- the person who is the subject of the information consents;
- the other purpose is directly related to the original purpose; or
- the use of the information for the other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of another person.

Exception to Principle 10:

- where the use is reasonably necessary for law enforcement purposes or the protection of public revenue;
- an investigative agency where compliance might interfere with investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- where an agency is authorised or required not to comply under any Act or law

## **Disclosure**

11. An agency must not disclose personal information to another body, including another public sector agency, unless:

- the purpose of the disclosure is directly related to the purpose for which the information was collected;
- the person concerned is reasonably likely to be aware, or has been made aware, that information of that kind is usually disclosed to the body; or
- the agency 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 person concerned.

Exceptions to Principle 11:

- where disclosure is made in connection with proceedings for an offence or for law enforcement purposes;
- where disclosure is made to a law enforcement agency to locate a person who has been reported to the Police as missing;
- where disclosure is authorised by a subpoena, search warrant or statutory instrument;
- where disclosure is reasonably necessary for the protection of public revenue;
- where disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed;
- an investigative agency where compliance might interfere with investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- where the individual expressly consents;
- any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier.

**12.** An agency should only disclose personal information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership if disclosure is necessary to prevent or lessen a serious and imminent threat to the person's life or health or that of another person.

Exceptions to Principle 12:

- where disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed;
- where an agency is authorised or required not to comply under any Act or law;
- where the individual expressly consents;
- any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier.

## **Privacy - Appendix B**

### **LEGISLATION AFFECTING PROCESSING OF INFORMATION**

#### **Legislation with General Application**

**Freedom of Information Act 1988:** deals with applications for access to cost centre documents which may contain personal information and applications for amendment of operational records of information relating to the personal affairs of the applicant. The Act creates an alternative means of accessing personal information but the Department may use limitations and conditions affecting access under the *FOI Act* when responding to applications for access and correction made under the *Privacy and Personal Information Protection Act*.

**Independent Commission against Corruption Act 1988:** defines corrupt conduct in a way which has been found to relate to unauthorised disclosures of information for personal benefit.

**Privacy and Personal Information Protection Act 1998:** in addition to the requirements covered in this Plan the Act prohibits disclosures of personal information by public sector officers which are not done in accordance with the performance of their official duties. These provisions are primarily directed against corrupt or irregular disclosure of personal information staff may have access to at work and not to inadvertent failure to follow policies and guidelines.

**Protected Disclosures Act 1994:** the definition of personal information under the *Privacy and Personal Information Protection Act* excludes information contained in a protected disclosure. This means that a person cannot seek review of the use or disclosure of a protected disclosure or be prosecuted for unauthorised disclosure of protected disclosure information under the *Privacy and Personal Information Protection Act*. However, the Privacy Management Plan is still able to address strategies for the protection of personal information disclosed under the *Protected Disclosures Act*.

**State Records Act 1998:** defines the circumstances under which the Department can dispose of its records and authorises the State Records Authority to establish policies, standards and codes to ensure adequate records management by the Department. Compliance with requests to delete irrelevant, inaccurate, or out-of-date information under section 15 of the *PPIP Act* appears to override the restrictions on destruction under the *State Records Act* (section 20(4)).

## **The Tribunal**

The *Privacy and Personal Information Protection Act* does not relate to the exercise of judicial functions by courts and tribunals. However, it does cover the handling of personal information in the exercise of administrative functions.

**Consumer Trader and Tenancy Tribunal Act 2001:** Part 2 relates to the establishment of the Tribunal, including the management of administrative functions. Part 5 relates to alternative dispute resolution.

**Consumer Trader and Tenancy Tribunal Regulation 2009:** Part 8 makes provision for access to Tribunal records.

## **Privacy - Appendix C**

### **POLICIES AFFECTING PROCESSING OF INFORMATION**

#### **Department Policies**

- Code of Conduct
- Policy for Use of Electronic Mail and the Internet
- Security of Information Systems Policy
- Security of Electronic Information Policy
- Draft Information Technology Strategic Plan

#### **External Policies**

The following external documents provide guidance on appropriate ways of collecting, storing, using and disposing of personal information:

#### **NSW Ombudsman's Office**

Ombudsman's Effective Complaint Handling Guidelines

#### **Office of Information Technology,**

IM&T Blueprint Memorandum Number 3.3: Security of Electronic Information available at <<http://www.oit.nsw.gov.au>>.

#### **Premiers Department**

Policy and Guidelines for the Use by Staff of Employer Communication Devices

(defines the responsibility of public sector employees in relation to the use of the Internet and electronic mail, available at:

[http://www.premiers.nsw.gov.au/publications/pubs\\_dload/coms\\_pol/compol.htm](http://www.premiers.nsw.gov.au/publications/pubs_dload/coms_pol/compol.htm)

The Public Sector Personnel Handbook August 1999

### **State Records New South Wales**

Destruction of Records: A Practical Guide, 1996

General Disposal Authority Administrative Records

(authorises routine disposal of commonly held categories of administrative records in accordance with approved schedules)

General Records Disposal Schedule - Personnel Records 1992

(authorises routine disposal of commonly held categories of personnel records in accordance with approved schedules)

### **Third Report of the AUSTEL Privacy Advisory Committee**

Calling Number Display,

(Attachment C Guidelines for Organisations using Caller ID available from the Australian Communications Authority Web site)

<<http://www.aca.gov.au/consumer/reports/cnd/index.html>>

### **Australian Communications Industry Forum**

Guideline Participant Monitoring of Communications, July 1998

(recommends conduct to be followed by organisations which monitor phone calls between employees and clients)

### **Privacy Committee**

Telephone Information Monitoring Systems, 1983

(establishes principles for recording employee calls. The Guidelines have been identified by Privacy NSW as in need of review to reflect new call recording and billing technology).

## **Privacy - Appendix D**

### **PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998**

#### **Procedures For Conducting Internal Reviews**

##### **1. Initial Discussions**

**1.1.** The CTTT has a policy of providing all reasonable assistance to anyone wishing to complain about the CTTT's handling of their personal information. It should be noted that most information kept by the CTTT relates to the hearing and determination of proceedings before it, and these functions are not affected by the *Privacy and Personal Information Protection Act 1998*.

**1.2.** The assistance will include, in the first instance and where possible, access to and correction of personal information without the need for recourse to formal internal review procedures.

**1.3.** Where a person, after discussion with the responsible officer, remains concerned or dissatisfied and wishes to proceed with a formal application for internal review the following procedures will be undertaken.

## **2. Application Forms for Internal review**

**2.1.** Applicants for internal review are assisted in the completion of their applications by the provision of an application form which ensures that all of the information required to constitute an effective application is obtained from the applicant.

**2.2.** A copy of the form, which is in the format suggested by the Office of the Privacy Commissioner, is attached.

## **3. The Internal Review Process**

**3.1.** In these procedures the term "responsible officer" means an officer who is qualified to deal with the subject matter of the complaint, by reason of the officer's seniority and experience, and who was not involved in the subject matter of the complaint.

**3.2.** On receipt of the application for review, the responsible officer will notify the Privacy Commissioner of the application and keep the Privacy Commissioner informed of the progress of the internal review. A review must be completed as soon as practicably reasonable and if not completed within 60 days from the date of receipt of the application, the applicant has a right to seek a review of the conduct by the Administrative Decisions Tribunal.

**3.3.** The responsible officer will assess the application to determine whether the review will be undertaken by the CTTT or whether it will be undertaken by the Privacy Commissioner. Matters which will influence this assessment will include whether the applicant has made a specific request for the review to be undertaken by the Privacy Commissioner or whether review by the CTTT could reasonably give rise to a perception of conflict or bias. Generally, preference will be given to the review being undertaken by the CTTT.

**3.4.** Following assessment, the officer will inform the applicant in writing of the name, position and contact telephone number of the officer conducting the review or of the fact that the review has been referred to the Privacy Commissioner, if applicable. This advice will also include information about the timeframe for completing the review and the range of actions the CTTT may decide to take in resolving the complaint. These include:

- take no further action;
- make a formal apology;
- take appropriate remedial action;
- give an undertaking that the conduct will not recur;
- implement measures to prevent recurrence of the conduct.

**3.5.** The responsible officer will take the following steps in the completion of the review:

- Assist the applicant to provide all relevant information and documentation in support of the complaint, including the particulars and evidence of the alleged breach and the harm, if any, caused by the alleged breach;
- Interview relevant staff and examine records and obtain any other pertinent information on the circumstances of the alleged breach;
- Identify the nature of the breach within the terms of the Privacy and Personal Information Protection Act, that is, whether the alleged conduct breaches an Information Protection Principle, a Code of Practice or a public register provision of the Act;
- Seek advice from the Office of the Privacy Commissioner, if required;

- Determine whether a breach has occurred and, if so, what harm or damage it has caused to the applicant;
- Prepare a report to the Registrar of the CTTT setting out the steps taken in the review, the conclusions reached and a recommendation for action to be taken to resolve the complaint. Letters to the applicant and to the Privacy Commissioner will accompany the report advising of:
  - the findings of the review and reasons for the findings;
  - the action proposed to be taken and reasons for that action;
  - the applicant's right to have the findings and the reasons for the findings reviewed by the Administrative Decisions Tribunal.

**3.6.** The responsible officer will also advise the applicant in writing of the status of the review if the complaint is not resolved within 30 days of the date of the application.

#### **4. Statistical Information on Applications and Outcomes**

**4.1.** The CTTT will maintain, in secure storage, statistical information on all applications for internal review and the outcomes of those applications for inclusion in the CTTT's Annual Report and for the information of the Privacy Commissioner.

#### **5. External Review**

**5.1.** People may apply to the Administrative Decisions Tribunal for a review of the action taken by the CTTT in conducting its review. The Tribunal may make orders requiring the CTTT to:

- Refrain from conduct or action which breaches an Information Protection Principle or Code;
- Perform in compliance with an Information Protection Principle or Code;
- correct information disclosed by the CTTT;
- take steps to remedy loss or damage;
- refrain from disclosing information in a public register.

**5.2.** The Tribunal may also make an order requiring the CTTT to pay damages of up to \$40,000 for loss or damage suffered where the conduct complained about occurs 12 months after the commencement of the internal review provisions of the Act (1 July 2000) where the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

Your concerns should be sent to the Chairperson or Registrar at the following address:

**Consumer, Trader and Tenancy Tribunal  
GPO Box 4005  
Sydney NSW 2001**