CORRUPTION AND CRIME COMMISSION
OF WESTERN AUSTRALIA

PROTECTING PERSONAL DATA IN THE PUBLIC SECTOR

Report of an Inquiry into Unauthorised Access and Disclosure of Confidential Personal Information Held on the Electronic Databases of Public Sector Agencies

September 2005

ISBN 0 9757248 4 3

This report and further information about the Corruption and Crime Commission can be found on the Commission's website at www.ccc.wa.gov.au

Corruption and Crime Commission

Postal Address	PO Box 7667 Cloisters Square PERTH WA 6850
Telephone	(08) 9215 4888 1800 809 000 (toll free for callers outside metropolitan Perth)
Facsimile	(08) 9215 4884
Email	info@ccc.wa.gov.au
Office Hours	8.30 am to 5.00 pm, Monday to Friday

Hon Nicholas Griffiths MLC
President
Legislative Council
Parliament House
PERTH WA 6000

Hon Fred Riebeling MLA
Speaker
Legislative Assembly
Parliament House
PERTH WA 6000

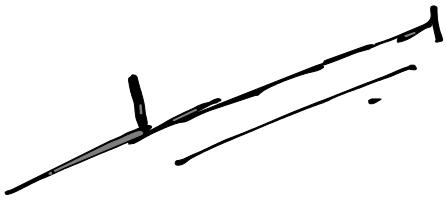
Dear Mr President
Dear Mr Speaker

In accordance with section 84 of the *Corruption and Crime Commission Act 2003* I am pleased to present the Report of the Corruption and Crime Commission's Inquiry into '*Unauthorised Access and Disclosure of Confidential Personal Information*'.

The opinion and recommendations contained in this report are those of this Commission.

I recommend that the report be laid before each House of Parliament forthwith pursuant to section 93 of the *Corruption and Crime Commission Act 2003*.

Yours sincerely



Kevin Hammond
COMMISSIONER

29 September 2005

CONTENTS

Executive Summary

The need for this Inquiry

The manner by which government agencies collect, categorise, store, retrieve and dispose of information has changed dramatically with the advent of electronic information technology. Whereas paper-based information systems have inherent limitations on the exchange of information, the migration of records to electronic format has greatly increased their ease of transfer.

While this increased ease afforded by computers raises concerns about the heightened potential for misuse of information in general, it is in regards to the privacy of personal information that perhaps the greatest concerns are held. Although 'hackers' using the Internet are frequently cited as the centre of concerns about unauthorised access of information, it is the opinion of the Corruption and Crime Commission (the Commission) that the leakage or loss of information through staff of the employing agency is a matter of far greater concern.

There is sophisticated technology available to help protect computer systems from incursions by external parties – including firewalls and virus, worm and spy ware protection. The same cannot be said for protection from internal unauthorised access and disclosures. Whereas we are intuitively guarded against external parties, we are more relaxed and confident with our own employees, trusting that they will do the right thing. It is the view of this Commission that this trust is at times misplaced.

The catalyst for the Inquiry

Since commencing in January of 2004, the Commission has received a steady stream of complaints and notifications regarding the unauthorised access of information held on the electronic databases of public sector agencies, and the disclosure of that information. Some of these complaints have been of a quite serious nature. The range of matters brought to the attention of the Commission indicates that this is not a problem that is only occurring in one or two agencies, or that it is errant behaviour of a few isolated individuals. Rather, the issues involve weaknesses in information management systems, the selection and management of staff who have access to information, and in the mechanisms available to deal with non-compliance. This has implications right across government.

Inquiry methods

On 5 November 2004, the Corruption and Crime Commission made a proposition that, in relation to the unauthorised access and disclosure of confidential personal information held on computer databases of public sector agencies, misconduct was occurring. Accordingly, it was decided to undertake an inquiry to look at aspects of:

- the legislative and policy framework for dealing with unauthorised access and disclosure of confidential personal information;

- arrangements for the selection and supervision of staff with access to personal information of a sensitive or confidential nature; and
- the awareness of staff of their responsibilities to safeguard confidential personal information.

Written submissions were solicited from members of the public through notices in the newspapers (11 received) and from a number of government agencies (six received). Specific information was also gained from several sample agencies, which was tested through fieldwork in those sample agencies.

Staff awareness and attitudes were gauged through the administration of a survey to 545 public officers (296 respondents).

First term of reference – Legislation and policy

Legislation

The main legislation relating to unauthorised access and disclosure and with the broadest reach are sections 81 and 440A of the *Criminal Code*, but there are problems in applying these sections. Advice from the Public Sector Investigation Unit of the Western Australia Police and the Director of Public Prosecutions highlights that these provisions are rarely, if ever, used.

Action against transgressing public officers may also be taken under the disciplinary provisions of the *Public Sector Management Act 1994*. However, multiple reviews undertaken under the auspices of the Department of the Premier and Cabinet have found that the statutory arrangements provided by this Act are overly prescriptive, too procedurally focussed, and do not allow disciplinary breaches to be dealt with efficiently. Furthermore, the provisions of this Act are largely restricted to public service officers with a great many public sector employees falling outside the Act's scope – although some are covered under other legislation.

Without a straightforward legislative basis for dealing with those who breach confidentiality, agencies often allow the employee to simply resign. This leaves the officer free to seek further employment with other public sector agencies which are unaware of this history. It also minimises the likelihood that the extent of misconduct of this type is identified formally and addressed as a systemic problem.

The Western Australian public sector needs legislation that provides a robust framework for the sanctioning of unauthorised access and disclosures both through criminal processes where warranted, and through disciplinary processes for less serious matters. Changes are necessary to legislation to ensure that the people of Western Australia can be confident that the information about them which is held by government agencies is secure and only used for its intended purpose.

Policy

The range of policy and procedures that has been developed by the public sector and which applies to the topic of this Inquiry is extensive. It is so extensive that, if not excusable, it is at least understandable that agencies may not be fully abreast of all of the overlapping requirements generated by these policies. It would appear that as each new problem arose it was responded to by the drafting of policy and procedures to address that particular concern without due regard for the overall state of the policy environment.

Second term of reference – Staff selection and supervision

Staff selection

Agencies at Commonwealth level and increasingly at State level are using background checks at the time of recruitment as part of the process of discerning the suitability of an applicant for a particular position. In Western Australia, this has generally involved a Western Australia police clearance or, since 2002, a National Police Clearance. These are based on the records held by each of the State and Territory police services together with those of the Australian Federal Police. It does not include prosecutions undertaken by agencies, other than police, under legislation other than the respective criminal law. Such prosecutions might be particularly relevant to the work-related responsibilities of the officer concerned, but they are not necessarily disclosed.

Supervision

The Inquiry Team found that the supervision of staff with access to confidential information was somewhat *laissez-faire*. It found few examples of computer systems with adequate audit tracking capability or that search for and identify anomalous accessing, other than in response to a specific complaint.

Third term of reference – Staff awareness

Staff of the sample agencies were tested on their awareness of their responsibilities and their perceptions of unauthorised access and disclosure of confidential information by way of a survey. This survey showed that staff of the sample agencies were reluctant to report an unauthorised disclosure to their supervising officer or other person. This occurred where the information was used to protect a third party or to 'right a wrong' or to serve some 'noble cause'. A view was also detected whereby staff who have access to information in the course of their work have a belief that they are somehow entitled to use that information for their own purposes.

All the sample agencies examined during this Inquiry included responsibilities to protect confidential information in their staff induction program, but often quite superficially, and each had policies related to the protection of such information. However, there was little evidence that employees had taken part in any induction program.

The Commission's recommendations

This report contains a number of recommendations that are to be found at the end of each relevant chapter, and are consolidated in the final chapter. The following recommendations are the most significant:

- The *Criminal Code* be amended to consolidate information security and privacy requirements, currently dispersed across more than 100 Acts, to prohibit unauthorised access and disclosure at every point in the distribution chain, and to clarify that an authorised user can also be guilty of unauthorised use.
- The disciplinary arrangements contained within the *Public Sector Management Act 1994* be repealed and replaced with a system that reflects 'normal' employment laws together with appropriate opportunity for review to ensure fairness of application.
- A consolidated approach and a coordinating authority are necessary to ensure that policies developed across government and over time are consistent and workable.
- Agencies improve the background checking of prospective staff, as a component of determining their suitability for employment by adopting the Commonwealth Protective Security Manual.
- Agencies adopt pro-active measures to reduce the opportunities for unauthorised disclosures rather than responding to individual incidences in isolation.
- Agencies ensure that their staff are aware of their responsibilities to safeguard confidential personal information entrusted to them through the development of policy that is relevant, and which is communicated to them at commencement of employment and regularly thereafter. This should include the introduction of a public sector oath or affirmation to maintain confidentiality of information, and the inclusion of relevant provisions in agency-specific codes of conduct.
- Government give immediate consideration to the implementation of the foreshadowed privacy legislation.

Subsequent reviews

The Commission, having made a number of recommendations within this report, will review the degree to which their implementation has made a difference in three years time.

Introduction

Extent of the problem

The exact extent of the problem of misuse of computer systems through unauthorised access and disclosure is not known and it is widely suspected that a great deal goes undetected. The anecdotal advice of those working in this area suggests that unauthorised access and disclosure occurs a great deal more than is ever officially reported or acted upon. This may be occurring for a number of reasons, including:

- Unauthorised accesses are difficult to detect as often it is only the parties to the accessing who are aware that it has taken place, with the person whose confidential personal information has been accessed remaining oblivious and therefore unable to make a complaint.
- The absence of security controls and audit tracking capability conceals the offences taking place. When asked to explain their computer transactions, the common refrain from officers is that they cannot recall why they may have accessed the information, or that someone else must have used their computer/password in their absence. As Kennedy (2004) reported, 'even when what would seem to be compelling evidence is available that information has been accessed in circumstances that constitute unauthorised use, such standard responses make the prosecution of the officer difficult, time consuming and expensive'.
- Difficulties with the disciplinary provisions of the *Public Sector Management Act 1994* mean that agencies are reluctant to commence a process that is doubtful of success, likely to be protracted, and invariably costly. Preference is therefore given to encouraging the resignation of the perpetrator as a means of dispensing with the matter.
- In some circumstances agencies may decide, for publicity or reputational reasons, not to disclose that they have been subject to computer misuse. It is believed that this may in some way be linked to the difficulties in substantiating that an offence has taken place, such that the agency is happy enough for the 'problem to go away' through the resignation of the officer – who may be encouraged to do so.

These factors together with other information gleaned during the course of this Inquiry leads the Commission to the view that all that we are ever seeing is the 'tip', and that the 'iceberg' itself remains largely unseen and unknown.

Commission proposition

On 5 November 2004, the Corruption and Crime Commission made a proposition that, in relation to the unauthorised access and disclosure of confidential personal information held on computer databases of public sector agencies, misconduct:

- has or may have occurred;
- is or may be occurring;
- is or may be about to occur; or
- is likely to occur.

This proposition was based on the Commission's own experience and knowledge, and made under the provisions of section 26 of the *Corruption and Crime Commission Act 2003 (CCC Act)*.

Having made this proposition, the Commission next made decisions in accordance with the provisions of sections 22, 32 and 33 of the *CCC Act*, and determined to undertake an investigation into this matter.

Terms of reference

The subject of this Inquiry was the 'unauthorised access and disclosure of confidential personal information held in the computerised databases of Western Australian public sector agencies'.

In particular, this Inquiry has focussed on the adequacy of:

- the legislative and policy framework for dealing with unauthorised access and disclosure of confidential personal information;
- arrangements for the selection and supervision of staff who have access to personal information of a sensitive or confidential nature; and
- the awareness of staff of their responsibilities to safeguard confidential personal information.

For the purpose of this Inquiry, confidential personal information is given to mean information of the type that could serve to identify an individual either directly or indirectly. This includes, but is not limited to, such information as:

- Personal details – name, address, telephone numbers, e-mail address, etc;
- Financial details – credit card number, bank account number, credit history, etc;
- Medical history; and
- Criminal history.

Methodology

The following methods were used in the Inquiry's information collection plan:

- Literature review to establish global legislative and policy frameworks for public sector agencies;
- Serving of s. 95 Notices under the *Corruption and Crime Commission Act 2003* requiring sample agencies to provide a range of corporate and operational documentation, policies, procedures, etc;
- Survey of staff attitudes towards disclosure scenarios;
- Call for written submissions from members of the public and identified government agencies; and
- Fieldwork to test whether the legislative and policy frameworks of the public sector were being implemented appropriately at an operational level.

Perceptions of misconduct survey

Determining the adequacy of public officers' awareness of responsibilities to safeguard against unauthorised access and disclosure was arrived at in part through the administration of a survey designed to identify staff perceptions of misconduct in relation to ten constructed scenarios. The survey document drew upon previous Australian research on ethics and perceptions of misconduct.

The survey required respondents to consider the scenarios involving unauthorised access and disclosure and to indicate the seriousness of each of the disclosures and whether they would report it or not. The scenarios were drafted with reference to:

- Actual complaints made to the (former) Anti-Corruption Commission and to the Corruption and Crime Commission; and
- Scenarios used in similar previous surveys.

The scenarios used in the survey instrument can be found in the chapter Perceptions of Misconduct Survey Report.

The survey was administered to 545 employees of the sample agencies with 296 completed surveys returned – a response rate of 54%

Submissions

Written submissions were solicited by way of a notice in *The West Australian* newspaper and nine regional newspapers and on the Commission's website. Additionally, key public sector agencies were specifically requested to provide a submission on aspects of the Inquiry. This resulted in 17 submissions being received, 11 from the public and six from government agencies. A list of submissions received is at Appendix 1.

While small in number, submissions from members of the public evidenced the hurt and damage that can occur when people believe that they have had their personal information disclosed in circumstances contrary to their interests. The matters they spoke of showed a consistency in that:

- they often had a lengthy history;
- they had previously sought satisfaction through a range of government agencies and ministers without success; and
- the chronologies of events and supporting documents provided with each submission combined to form a thick dossier running to many pages.

It was obvious that the people making the submissions felt strongly aggrieved by the perceived injustices perpetrated upon them, and that the matters had proven incapable of resolution by the agencies involved. Indeed, their dissatisfaction with the agencies and others they went to for relief frequently became themselves the subject of complaint. As a result, the complainants continued with efforts to gain satisfaction long past a time that many people would consider reasonable and to the point where any 'victory' achieved would be pyrrhic.

Submissions from the Auditor General, Director General of the Department of the Premier and Cabinet, Director of Public Prosecutions, Public Sector Standards Commissioner, Department of Education and Training and the Western Australia Police were of particular assistance in identifying flaws and deficiencies in the legislative and policy framework, and in drawing attention to previous reports and reviews on these matters.

Fieldwork

The fieldwork component of the Inquiry addressed the terms of reference by an examination of the legislation, policy, and procedures in use at the following six agencies:

- Department for Community Development
- Insurance Commission of Western Australia
- Department for Planning and Infrastructure
- City of Rockingham
- City of Melville
- Department of Justice – Maddington and Victoria Park Community Justice Services Offices

These sample agencies were selected on the basis of perceived risk, public interest, and in order to cover a range of information types and practices. Agency policies and practices were assessed against legislative requirements and identified good practice. This included good practice in relation to:

- Definition and classification of confidential and public information;

- Legislative and policy environment;
- Access to confidential personal information;
- Authorised disclosure of confidential personal information;
- Management of known instances of unauthorised access and disclosure;
- Selection and supervision of staff with access to confidential personal information; and
- Staff awareness of responsibilities.

It is appropriate to acknowledge the cooperation of the chief executive officers of these agencies and of their staff in giving of their time and in responding to requests for information and documentation. There was a view from the CEOs and senior managers of these agencies that they were pleased at the opportunity to assist in this Inquiry. Further, there was an interest in the outcome of the Inquiry to see if there were ways in which they could improve their respective operations. This cooperation and support was greatly appreciated.

Conduct of the Inquiry

The Inquiry into unauthorised access and disclosure of confidential personal information was undertaken by the Corruption Prevention, Education and Research Directorate of the Corruption and Crime Commission, with the Inquiry Team consisting of Glenn Ross, Karen Schmidt, Carolyn Simmonds, Tony Pruyn and Nadine Bernhardt.

With the exception of Mr Ross, all other members of the Inquiry Team were seconded from other agencies under the provisions of s. 181 of the *CCC Act* to undertake the Inquiry. The willingness of the home agencies to release these staff members for this purpose was greatly appreciated.

Legislative Framework

Introduction

The *Commission on Government Report No. 1* (1995: 43) identified in excess of 100 Acts and regulations in Western Australia that placed secrecy restrictions of some form or other on government departments and public bodies. In almost all cases the legislation deals with the subject in the context of two broader, often conflicting topics, namely privacy and transparency in government.

The relevant Acts and regulations differ in terms of their focus, what information is protected, the types of access and disclosure they cover and the penalties they impose. The differences may well reflect different circumstances, but what those circumstances are and why they should result in different rules and penalties is not always apparent.

The following legislation has the broadest reach and is of greatest interest to this Inquiry:

- *Criminal Code Act Compilation Act 1913 (Criminal Code)*; and
- *Public Sector Management Act 1994 (PSM Act)*
- *Freedom of Information Act 1992 (FOI Act)*
- *State Records Act 2000 (SR Act)*

Some legislation is either agency specific or topic specific. The Inquiry looked closely at the *Local Government Act 1995 (LG Act)* as it covers two of this Inquiry's sample agencies. Also included in this section is reference to a number of agency/topic specific legislation that has been included to give an appreciation of the widespread and often overlapping nature of much of the legislative content.

The differing jurisdictional coverage of these Acts and the differing definitions employed makes comparisons difficult and cumbersome. Some relate to the broader public sector[1] while others have a narrower focus to the public service,[2] and establishing whether a particular agency is covered by a particular Act can be difficult. Similarly, the differing definitions for similar terms adds to the complexity and confusion. There is overlapping legislation such that a transgressor may be guilty under a number of Acts and, depending upon which is used, the penalties may differ markedly. While this is perhaps not a totally unknown situation, it is not helpful to those required to administer the legislation.

[1] Includes local government, universities, and a large range of government business entities, etc.
[2] Relates more narrowly to government departments such as Health, Education and Justice, etc.

The Criminal Code

Section 81

The offence of 'disclosing official secrets' is to be found at s. 81(2) and applies where a person without lawful authority makes an unauthorised disclosure, and carries a penalty of imprisonment of three years. On summary conviction, however, the penalty is imprisonment for 12 months and a fine of $12,000.

Unauthorised disclosure is defined in the Code to mean the disclosure, by a person who is a public servant or government contractor, of official information in circumstances where the person is under a duty not to make the disclosure.

The Code defines the underlined terms as follows:

Public servant means a person employed in the Public Service.[3] The Public Service itself is defined in the *Public Sector Management Act 1994* as being constituted by departments and SES organisations (where posts or persons employed in them belong to the Senior Executive Service) and persons employed under Part 3 of that Act.

Government contractor means a person who is not employed in the Public Service but who provides, or is employed in the provision of, goods or services for the purposes of:

- the State of Western Australia;
- the Public Service; or
- the Police Force of Western Australia.

Disclosure includes '*any publication or communication and, in relation to information in a record, parting with possession of the record*'. Thus, a public servant who obtains unauthorised access to information, but makes no use of it, does not commit an offence under this section of the *Criminal Code*.

Information is quite broadly defined to include false information, opinions and reports of conversations, while *official information* means 'information, whether in a record or not, that comes to the knowledge of, or into the possession of, a person because the person is a public servant or government contractor'.

The Code does not say when the '***duty not to make a disclosure***' might arise. While policy statements and codes of conduct play significant roles in defining the parameters for good practice in relation to the handling of confidential personal information, they are not definitive. It is not entirely clear when a public servant has a 'duty' to keep secret certain information. As an example, *Pense v Hemy* [1973] WAR 40 is a useful reference on the difficulty of determining a police officer's duty to keep information secret.

[3] s. 81(1)

In terms of the usage that is made of s. 81, the Director of Public Prosecutions has advised by submission that there have been very few prosecutions pursuant to that section of the *Criminal Code*. On the few occasions where this has occurred, it has primarily involved unauthorised disclosure by police officers.

Section 82

Section 82 deals with the issue of bribery, in that, any public officer who obtains, or seeks or agrees to receive, a bribe, and any person who gives, or who offers or promises to give, a bribe to a public officer, is guilty of a crime and is liable to imprisonment for seven years. This includes the offering and receiving of a bribe to disclose unauthorised information.

Section 83

This section provides that, *inter alia*, any public officer who, without lawful authority or a reasonable excuse 'acts upon any knowledge or information obtained by reason of his office or employment … so as to gain a benefit, whether pecuniary or otherwise, for any person, is guilty of a crime and is liable to imprisonment for 7 years'. The definition of 'acts upon' is problematic, as in *Rompotis v R* (1996) 18 WAR 54 it was held that to 'act upon' information means more than merely communicating that information that has been obtained by virtue of official office. Further, in relation to gaining a benefit, unless the benefit is a financial one, there may be problems in substantiating that a benefit has actually been exchanged for the information (Criminal Justice Commission, 2000: ix–xiii).

The available evidence from this and other inquiries is that the expectation of monetary benefit is not the main precursor to the disclosure of information. Rather, it is frequently provided due to a relationship or friendship between the person seeking the information and the officer having access to it. In the absence of any proof of a benefit being received, the only evidence of an offence having been committed would be the possession of the provided information. Although there is currently no offence of being in possession of confidential information, there should be, much in the same manner as receiving stolen goods.

An inquiry conducted by the Independent Commission Against Corruption (NSW) in 1992 concluded that:

> Protected government information should be regarded as a prohibited commodity, like proscribed drugs or stolen goods. It should be an offence, not only for public officials to release it, but for others to buy or sell or otherwise deal in or handle it, or to disseminate it in any other way, without authority … and a reverse onus of proof once unexplained possession or handling is established.

This Commission shares this view.

Section 7

Section 7 provides that persons involved in an offence in the following ways are deemed to have taken part in committing the offence and to be guilty of the offence and may be charged with actually committing it:

- Every person who actually does the act or makes the omission which constitutes the offence;
- Every person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence;
- Every person who aids another person in committing the offence; and
- Any person who counsels or procures any other person to commit the offence.

This provision covers other parties to an offence and has application to those persons who solicit an unauthorised access or disclosure.

Section 440A

The *Criminal Code* at s. 440A concerns the offence of unlawful use of a restricted-access computer system, and provides a range of penalties in relation to the type of misuse. The main focus of this Inquiry involves situations where a person unlawfully uses a restricted-access computer system when not properly authorised to do so, or if authorised to use it, uses it other than in accordance with that authorisation.

The difficulties with the previously worded s. 440A , regarding the unlawful operation of a computer system, were well canvassed by Kennedy (2004) in his inquiry when he looked at unauthorised access and disclosure by police officers. Regarding the workability of s. 440A, in his submission to this Inquiry, the Director of Public Prosecutions advised 'In relation to section 440A of the *Criminal Code*, in my time as DPP I have never commenced a prosecution pursuant to this section'.

Included in the submission received from the Western Australia Police was advice from its Public Sector Investigation Unit that during the period 1 January 1999 to 31 October 2004, 115 police officers were investigated for unauthorised access and 219 for unauthorised disclosure. The most frequent outcome of these investigations was 'not sustained'. No officers were charged under the provisions of s. 81 or s. 440A of the *Criminal Code* for these offences.

Despite the provisions of sections 80–83 and 440A, there is no offence committed under the *Criminal Code* when a person who is an authorised user improperly accesses confidential personal information held on government databases. A report by the Criminal Justice Commission (2000: 105) included the submission of the Australian Privacy Charter Council that browsing should be an offence:

> Another recommendation we would have would be that it should not just be disclosure of confidential information that should be an offence but the mere browsing of a computer system should be detectable and should be made an offence if it's obvious that that's occurring for non-authorised reasons.

There is a view that use of the *Criminal Code* should only be made when dealing with the more serious of unauthorised access and disclosures. This might include where there has been an exchange of money or other considerations of value, or where a degree of maliciousness is associated with the disclosure. It is, however, accepted by this Commission that circumstances may arise whereby there is benefit in having 'browsing' included within the provisions of the *Criminal Code* – and it is so recommended.

There is an argument that can be made against extending the criminal offences in relation to unauthorised access and disclosure made via computer systems. For some, such extension would further extend the current anomaly whereby unauthorised accessing of information through computers is treated significantly differently from unauthorised access by means other than by computers. Unauthorised access, other than by way of a computer, is not in itself a criminal offence – some other offence such as trespass or theft must also be involved (Law Commission, 1999: 14). This argument is not persuasive. There is a strong public interest in protecting the community from misuse of computers such that it outweighs the concern about this anomaly.

Public Sector Management Act 1994

Through its General Principles of Public Administration and its Code of Ethics, the *PSM Act* effectively makes unauthorised access and disclosure a breach of discipline. Agency-specific codes of conduct, where they exist, are also likely to cover access and disclosure. However, these do not have the force of law.

The *PSM Act* at ss. 7–9 sets out three general operating principles that the public sector must observe. The principles cover the broad areas of:

1. Public Administration and Management;
2. Human Resource Management; and
3. Official Conduct.

Of importance to this Inquiry is the Official Conduct principle, which requires that, *inter alia,* all public sector bodies and employees are to act with integrity in the performance of official duties and are to be **scrupulous in the use of official information**, equipment and facilities (emphasis added).

Breaches of the *PSM Act* constitute a breach of discipline. Minor breaches are punishable by a reprimand, a fine or both. Serious breaches can incur the same penalties as well as a transfer, a pay reduction, a reduction in level, a combination of these, or dismissal.

The *PSM Act* at s. 3 defines a 'public sector body' to mean 'agency, ministerial office or non-SES-organisation' with 'agency' defined as 'a department or SES organisation'. 'Employee' has the meaning of a 'person employed in the Public Sector by or under an employing authority' and an 'employing authority' includes a Minister, a CEO, or a board, committee or other body established under a written law.

The net effect of these definitions is that, unlike the *Criminal Code*, these General Principles do not cover either contractors or their staff. By virtue of the definition of the 'Public Sector', the General Principles also do not cover elected officials (Members of Parliament and local government representatives) Parliament's employees, local government employees, police officers, staff of universities, any court or tribunal established under a written law, the staff of the Governor's establishment and Members of Parliaments' electorate offices.

The *PSM Act* has been the subject of a number of reports since its inception in 1994. Principal among these are the Fielding Report of 1996, the Kelly Report of 1997 and the Whitehead Report of 2004. There is a consistency in the recommendations of these reviews concerning the disciplinary component of the *PSM Act* – Part 5. Commissioner Fielding, a member of the Western Australia Industrial Relations Commission, concluded that:

> These provisions have been widely criticised as being too prescriptive and focusing too much on procedures rather than outcomes. Indeed so complex are the procedures that some chief executive officers indicated they had been discouraged from taking action against offending employees. Alternatively, where action was taken, in many instances it took so long as to be destructive of morale within the agency. (Fielding, 1996: 153–154)

The answer according to Fielding was to adopt the general employment laws applicable to those persons outside of the public service:

> The general employment law embodies rules and principles for dealing with complaints of substandard performance and breach of discipline. Those rules and principles are readily adaptable to the public sector. I recommend that the procedural provisions contained in the Act therefore be repealed and that the management of complaints relating to substandard performance and breaches of discipline be left to the general law. (1996: 7)

Fielding's proposal for the adoption of practices in keeping with 'normal employment law' would see the abolition of 'charging ' employees with breaches of discipline, a 'quasi-criminal' process, and its replacement with breaches of contract instead.

This view of Fielding is no orphan. Dr Des Kelly, as Chairman of the Working Party convened to consider the recommendations of Fielding, concurred with the recommendation of Fielding for the Act to '… [provide] only a general framework for disciplinary action in public sector employment – including reference to the application of the common law – with detailed prescription to be set down in Standards and approved procedures' (1997: 46).

In 2004 the *PSM Act* was again reviewed, this time by Mr Noel Whitehead. In relation to substandard performance and disciplinary matters, Whitehead reported that, based on submissions received and discussions held with various parties:

> … the current provisions in the Act are unnecessarily complex, can lead to extended and costly processes, and the requirement to comply with the various processes within the provisions of the Act places a considerable burden on employers to deal with matters in an expeditious manner.

Whitehead concluded that it was evident that the prescriptive nature of Part 5 of the Act was complex and unworkable and in need of redrafting.

Despite the recommendations by Messrs Fielding, Kelly and Whitehead, in repeated reviews, redrafting has yet to occur. This Commission supports these calls for a redrafting of the substandard performance and disciplinary sections of the *Public Sector Management Act 1994*.

Chief executive functions

Section 29 of the *Public Sector Management Act 1994* deals with the functions of chief executive officers and chief employees. It requires that the chief executive officer satisfy a broad range of management and leadership functions, with specific reference to requirements under the *Industrial Relations Act 1979*, *Occupational Safety and Health* Act *1984* and the *State Records Act 2000*.

It is contended that the issue of unauthorised access and disclosure is of such significance that this section should be amended to specifically include the responsibility for the protection of confidential personal information. Further, this responsibility should extend to providing staff with comprehensive guidelines and instructions together with appropriate training to ensure that staff are aware of their responsibilities to safeguard confidential personal information.

Public Service Regulations 1988

The submission from the Department of the Premier and Cabinet made reference to discussions that have taken place with the Commissioner for Public Sector Standards regarding the need to develop an appropriate disciplinary framework for dealing with unauthorised release of information. Particular concern was expressed at the continuing inappropriateness of regulation 8 of the Public Service Regulations 1988 and of Administrative Instructions 711 and 728.

Regulation 8 requires that:

An officer shall not:

(a) publicly comment, either orally or in writing, on any administrative action, or upon the administration of any Department or organisation; or

(b) use for any purpose, other than for the discharge of official duties as an officer, information gained by or conveyed to that officer through employment in the Public Service.

This regulation was criticised by the 1992 Western Australian Royal Commission into Commercial Activities of Government and Other Matters (WA Inc. Royal Commission) and subsequently by the 1995 Commission on Government. The criticisms of these commissions surround the 'blanket' nature of part (a) and the difficulties in determining the 'duties' in part (b), and were to the extent that the regulation was recommended for repeal.

While acknowledging the inadequacy and difficulties of this regulation, the Director General of the Department of the Premier and Cabinet is of the view that to repeal this regulation without replacement would create even greater difficulties. This is due to concern that the high-level statements contained within the WA Code of Ethics and the voluntary agency-specific codes of conduct would not in all cases provide clear grounds under which to take action. The recommendation therefore is for 'specifically targeted legislative provision' to achieve the desired outcome of a consistent approach.

The Director General has proposed that the *Public Sector Management Act 1994* may be a suitable mechanism for achieving this reform, although acknowledging that it suffers in that its application does not include many public sector agencies within its scope, particularly the large organisations listed in schedule 1 of the *PSM Act* (see Appendix 8).

Freedom of Information Act 1992

The *Freedom of Information Act 1992 (FOI Act*) creates a general right of access to state and local government documents, other than documents of exempt agencies. Exempt agencies are listed in Schedule 2 to the *FOI Act* and include independent agencies such as the Ombudsman and the Auditor General, and indeed this agency, and entities involved in the administration of justice, such as the Bureau of Criminal Intelligence of the Western Australia Police.

Although the *FOI Act* is primarily designed to encourage disclosure of information held by government, wherever it is reasonable to do so, the *FOI Act* also outlines a number of exemptions, which are designed to prevent disclosure where, for instance, it would have a detrimental effect on the function of the Government. One of the exemptions

(clause 3 of Schedule 1 to the *FOI Act*) expressly recognises the need to prevent disclosure of 'personal information', which it defines in the Glossary as:

- Information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead –
    - whose identity is apparent or can reasonably be ascertained from the information or opinion; or
    - who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.

The purpose of this exemption is to protect the privacy of individuals. Where a person seeks to obtain personal information about another person, the onus is on the access applicant to establish that disclosure of personal information about a third party would, on balance, be in the public interest.

A search of the FOI Commissioner's published decisions identifies that the Commissioner has consistently expressed the view that the public interest in protecting the privacy of individuals is strong and can only be displaced by some stronger countervailing public interest, which requires the disclosure of personal information about one person to another. To date, the Commissioner has not made a decision where it is considered that the public interest in protecting the privacy of individuals has been displaced by some stronger countervailing public interest

Of interest is that the definition of public body or officer under the *FOI Act* expressly includes 'a contractor or subcontractor' but other provisions limit this term to a very small sub-category of contractors, namely those that provide court security and custodial services or prison services. This is in contrast to the *Criminal Code* where the term 'contractor' has a much wider application.

State Records Act 2000

The *State Records Act 2000* (*SRA Act*) sets out a regime for the keeping of state records. It has established Minimum Compliance Requirements (MCR) to underpin the duty of all agencies to have approved Record Keeping Plans. One of these MCRs covers 'security and protection' and 'access to all records, in all formats'. It is understood that this has helped to raise the risk profile of both internal and external unauthorised access and disclosure, although not to the level that this Commission seeks.

The *SRA Act* also provides limited protection of personal information and therefore gives rise to rules relating to access and disclosure. The main limitation is that the protection relates to government records in the form of state archives, a term defined to mean records that are to be retained permanently. Where a government record is a State Archive as defined, and the record includes information about a person's medical condition or disability, the *SRA Act* states that no access is permitted unless the person consents, or the information is in a form that neither discloses nor would allow the identity of the person to be ascertained.

The *SRA Act* still needs to be considered here, because it requires government organisations to manage their record keeping according to certain principles which incorporate, either directly or through related MCRs, many of the good practice principles for preventing unauthorised access and disclosure. For instance, Standard 2 sets out six principles for ensuring government record keeping plans meet the requirements of s. 19 of the Act. Principle 2 requires agencies ensure that record keeping programs are supported by policy and procedures, and one of the related MCRs requires agencies to provide evidence their policies and procedures cover records in all formats and all aspects of their management, including:

- the creation of records;
- their capture and control;
- their security and protection;
- access to them; and
- their appraisal, retention and disposal.

Other MCRs related to Principle 2 require evidence that:

- Policies and standard operating procedures governing record keeping in the organisation are established, authorised at an appropriate senior level, and are available to all employees;
- The policies and procedures define the roles and responsibilities of all employees who manage or perform record keeping processes;
- The policies take into account relevant government policy and endorsed standards for the making and keeping of proper and adequate records;
- The organisational scope of the policies and procedures has been addressed, i.e. whether they are applicable to the entire organisation, including divisions, regional branches and offices and outsourced contractors; and
- The custodianship and management of government records has been addressed in regard to organisational restructures, the transfer of an organisation's functions, the creation of new business units or the devolution of authority for managing government records.

Principle 4 requires government organisations ensure that records 'are protected and preserved'. The related MCRs include requirements that agencies provide evidence that:

- The organisation has identified and assessed the risks[4] and impacts of disasters on its recorded information; and
- The organisation has planned strategies and activities for the reduction and management of risks to its records.

[4] The Self-Evaluation Checklist that agencies are required to complete and submit to the State Records Commission together with their Record Keeping Plan states that the assessment must be a systematic one covering a range of disasters including 'criminal behaviour and neglect', the likelihood of each disaster occurring (rated low to high) 'and the risks to the organisation's records, with particular regard to current storage facilities, including: onsite, offsite, including off-site use of records … and security and access'.

The *SRA Act* provides for a penalty of $10,000 for breaching confidentiality requirements or for failing to keep records appropriately. It is not known if any person has been convicted under this Act. The penalty applies only to a particular individual and not to the agency itself.

Local Government Act 1995

The *Local Government Act 1995 (LG Act)* contains two provisions relating to unauthorised disclosure. The more general provision (s. 5.93) prohibits council members, committee members and local government employees from making 'improper use of any information acquired in the performance by [them] of any of his or her functions under the Act or any other written law' for their own or anyone else's benefit or to cause detriment to the local government or any other person. The penalty is $10,000 or imprisonment for two years.

The *LG Act* does not define 'improper use' or 'information' but 'employee' is defined as a person employed by a local government under the *LG Act*. The Act is silent on contractors and their staff, suggesting that they are not covered.

The second provision relates solely to information in registers of financial interests. It prohibits anyone from publishing any information derived from a register unless the information constitutes a fair or accurate report or summary of information contained in the register and is published in good faith. It also prohibits any comment on the facts set forth in the register unless the comment is fair and published in good faith.

The penalty in both cases is $5,000 or imprisonment for one year. The term 'publish' is defined as having the same meaning as it has in the *Criminal Code* in relation to the publication of defamatory matter.

The *LG Act* at s. 5.103 also requires every local government to adopt a code of conduct to be observed by council members, committee members and employees. The Western Australian Local Government Association drafted a Model Code of Conduct for elected members in 1996, which it is understood was adopted by local governments, in most cases, without amendment. The Association has conducted a review of the Model Code, and identified the unenforceability of the Model Code as a major concern. They resolved that enshrining a minimum code into regulations would be the preferred mechanism for alleviating this concern.

Other legislation

Other state laws include secrecy or non-disclosure provisions. Public sector employees may also be bound by other laws but in most cases these laws are much more circumscribed – the duties tend to be limited to people with certain professional qualifications, or who carry out a particular function or activity, or are agency specific.

Several of these laws are reported here to evidence the array of legislation that concerns this important area of public policy.

Health Act 1911

This Act includes a number of provisions protecting disclosure of two types of personal information – that relating to venereal diseases and disorders affecting the generative organs and information obtained in the administration of environmental health matters such as control of food cultivation, food premises, food vehicles, appliances and food vending machines. There are also a number of provisions limiting access and disclosure of results of investigations of perinatal and infant mortality and maternal mortality, and identifying information provided for medical research purposes generally as well as contained in reports on investigations of perinatal and infant mortality and maternal mortality.

Financial Brokers Control Act 1975

Section 88(2) prohibits the release of '... any information concerning the affairs of any other person'. The duty is limited, however, to 'any person who is, or has been, a member or the deputy of a member, or the Registrar, an inspector, or any other officer, whether permanent or temporary, of the (Finance Brokers Supervisory) Board'. The reference to 'officer' indicates that the duty does not cover contractors and their staff.

Equal Opportunity Act 1984

Section 167 prevents the disclosure of 'any information relating to the affairs of another person'. The duty is limited, however, to past and present Commissioners and staff of the Tribunal although it does appear to extend to contractors. The penalty for breach is $2,500.

Human Reproductive Technology Act 1991

Section 49 prohibits anyone disclosing certain types of information – the identity of donors of gametes or eggs or a participant in any procedure involving reproductive technology or a child born as a result of any artificial fertilisation procedure, except for certain research, medical, or administrative purposes or with the consent of the person identified or where authorised under another written law. The penalty is $5,000 or imprisonment for 12 months.

Disability Services Act 1993

Section 52 prohibits, with some exceptions, past and present members of the Board of the Disability Services Commission, Commission personnel, other government staff used by the Commission, contract staff and service providers, 'whether directly or indirectly, recording, disclosing, or making use of any information obtained' by virtue of their position.

The exceptions cover disclosure in the course of duty, or as required or allowed by the Act or any other law, or where it is in the public interest to protect the physical safety of an individual, for certain formal investigations, or with the consent of the person to whom the information relates, 'or in prescribed circumstances'. The penalty for breach is $2,500.

Health Services (Conciliation and Review) Act 1995

This Act establishes an agency to handle complaints about the provision of health services. Section 71 creates an offence similar in form and structure to s. 52 of the *Disability Services Act* in that it covers past and present staff of the agency. It also covers anyone involved in conciliation or investigation of the complaint or to whom the complaint is referred or who receives a formal notice under the Act. The prohibition and exceptions are similar except, in relation to the latter, a person to whom the information relates must provide their consent in writing. The penalty for breach is $2,500.

Mental Health Act 1996

The offence set out in s. 206 is also similar in form and structure to s. 52 of the *Disability Services Act*. The exemptions are similar except that they expressly cover the situation where more than one person is identified in the information. In this case it states that each of them must consent to its release but there is no requirement that the consent must be in writing. The prohibition also 'does not apply to the divulging of statistical or other information that could not reasonably be expected to lead to the identification of any person to whom it relates'. The penalty for breach is $2,000 or imprisonment for six months.

Agency responsibility

In addition to legislation and policy that proscribes the behaviour of individual public officers, the Auditor General made the point in his submission that agencies also have a responsibility:

> … it is important that legislation and policy is effective in governing the mechanisms for the public sector to disclose personal information. It is also important that relevant legislation outline the provisions for prosecution and penalties for those **agencies** who fail to adhere to proper practice in this area. Not only must it be clear what penalties exist, but which authority is accountable for monitoring compliance and bringing any breaches to prosecution. Clarity in legislation and policy will maximise the capacity for accountability officials such as the Auditor General to fulfil their mandate effectively (emphasis added).

Whereas in regard to private sector organisations there are many examples of legislation that applies penalties to an organisation that breaches legislative provisions, this is not the case with public sector agencies. In many circumstances the ability of an individual employee to make an unauthorised access and disclosure is due to inherent weaknesses in the systems of an agency. All agencies ought to be aware by now of their responsibilities to protect the confidential personal information of their clients, and be taking the necessary steps to ensure such protection. Where they have failed to do so, those responsible within the agency should also be brought to account.

The *Occupational, Safety and Health Act 1984* (*OHS Act*) is of interest as a potential model in that it contains requirements and penalties applicable to both the employer and the employee. Section 19(1) relates to duties of employers to, in the simplest terms, provide

a safe working environment; provide information, instruction and training; and take other relevant action. If an employer contravenes s. 19(1) they commit an offence, which, dependent upon the circumstances, attracts a penalty ranging from a level two penalty to a level four penalty.

In regards to employees, s. 20(1) requires employees to, again in the simplest terms, work in a safe manner and avoid adversely affecting the safety or health of others through act or omission. Failure to do so can lead to a penalty of $25,000 in the first instance and $31,250 for offences thereafter.

This mutual commitment of both employer and employee contained in the *OHS Act* and the ability to level penalties against employers and employees alike may well have application to the problem of unauthorised access and disclosure. While efforts to date have centred on gaining the compliance of the employee to work in a particular manner and to punish them when they do not do so, there is no comparable requirement on an agency to do its part to provide an environment that mitigates such disclosure occurring – perhaps there should be.

Adequacy of the legislative framework

To ensure the right level of protection is afforded to confidential personal information it is necessary that stronger support be obtained from the law. This is particularly so in the post-9/11 society, where governments are reconsidering such things as a national identity card and other extensions to information holdings on individuals. It is unlikely that the community will happily embrace such measures unless it is confident that the new information to be gathered and stored will be safe. It is not possible, at present, to give the community that assurance and confidence, as confidential personal information in the hands of the public sector is not as secure as it ought to be.

The legislation examined in this report evidences a number of problems. The lack of consistency in terminology related to information security and secrecy provisions, and to definitions in relation to public officers, etc. and to the jurisdiction over which the various Acts have coverage leads to confusion. Furthermore, there is a lack of consistency and an unacceptably broad continuum in terms of penalties and criminal sanctions for breaches. The variance in penalty ranges from $500 in the *Finance Brokers Control Act 1975* to $5,000 in the *Human Reproductive Technology Act* and to seven years imprisonment under the *Criminal Code*.

It is appreciated that these information protection provisions have developed in a piecemeal fashion in response to specific concerns in the relevant agencies or areas of public policy. It is timely that these disparate pieces of legislation be reconsidered and, where possible, consolidated.

In combination, sections 7, 81, 82 and 83 of the *Criminal Code* would appear to be adequate provisions to address conduct of unauthorised accessing and disclosing of confidential personal information. However, as was also the opinion of Kennedy (2004), there is need for improvement. Also in need of improvement are the disciplinary

provisions relating to public sector employees employed under the *PSM Act*. Information given to this Commission is strongly suggestive that agencies are not inclined to use these provisions due to their complexity and unlikelihood of success.

Recommendations – The Criminal Code

The Commission recommends the amendment of the *Criminal Code* to consolidate offence provisions relating to unauthorised access and disclosure and to create a uniform set of provisions to address the inconsistencies of jurisdiction, definitions and penalties that currently exist. In seeking amendments to the Code the Commission further recommends that:

- Offences of unauthorised access and disclosure should prohibit dealing in the outcomes of unauthorised access at every point of the distribution chain, and include:

  - Unauthorised access;
  - Unauthorised use including 'browsing';
  - Unauthorised disclosure;
  - Procuring or bringing about unauthorised access or disclosure;
  - Attempting to procure or bring about unauthorised access or disclosure;
  - Soliciting or inducing another to make unauthorised access or disclosure;
  - Offering to make unauthorised access or disclosure;
  - Promoting oneself as capable of supplying information through unauthorised access or disclosure;
  - Being in possession of confidential information without benefit of an excuse (with a reverse onus applying); and
  - Buying selling or otherwise dealing in confidential information.
  - Persons at second or third hand who gain access to unauthorised confidential personal information, knowing or ought to be knowing that it was made available through unauthorised access or disclosure.

- Unauthorised access and disclosure provisions are extended to embrace contractors and sub-contractors who are providing a service to a public sector agency and have access to confidential personal information as a consequence.
- Unauthorised access and disclosure provisions are extended to embrace volunteers, placement and practicum students and other similar unpaid persons while performing duties as public officers and who have access to confidential personal information in the course of these duties.
- In redrafting the *Criminal Code* the opportunity should be taken to clarify that a person who is an authorised user of a computer system can still be an unauthorised user if access is made beyond the scope of the authorised access.

Recommendations – Public Sector Management Act 1994

The Commission recommends the amendment of the *Public Sector Management Act 1994* to enable matters of unauthorised access and disclosure to be dealt with more appropriately. In seeking amendments to the *PSM Act* the Commission further recommends that:

- The substandard performance and disciplinary sections (Part 5) of the *PSM Act* be redrafted to bring them into keeping with contemporary employment law and practices.
- Legislation be enacted to make public sector agencies not currently subject to the *PSM Act 1994* subject to the *PSM Act* for disciplinary purposes. Section 239 of the *School Education Act 1999* provides a useful model:

  > *Part 5 of the PSMA has effect as if in that Part references to:*
  >
  > *(a) an employee included –*
  > *(i) a member of the teaching staff; and*
  > *(ii) an officer who comes within section 235(1)(c); and*
  >
  > *(b) an employing authority that is not the Minister (within the meaning in that Part) included references to the chief executive officer.*

- Clarification be made of the duty of public officers to maintain confidentiality of confidential personal information to better bring unauthorised disclosure within the provisions of s. 81 of the *Criminal Code*.
- An obligation is created for public sector agencies to provide an environment that mitigates the disclosure of confidential personal information through amending s. 29 of the *PSM Act* to specifically include a chief executive officer's responsibility for the protection of confidential personal information held by their agency.

Recommendations – Other legislation

In relation to other legislation, the Commission recommends that:

- Once the recommended amendments have been made to the *Criminal Code*, the existing provisions in agency- or area-specific legislation should be repealed in preference to the *Criminal Code*.
- The *Local Government Act* be amended to include a compulsory minimum code of conduct, the breach of which would constitute a disciplinary offence.
- Regulation 9 of the Public Service Regulations be repealed once the *PSM Act* has been amended as recommended.

Policy Framework

Introduction

A number of informal laws or non-statutory rules are relevant to the Inquiry. There are many different types of these, most designed to provide guidance, consistency and good governance. They may be embodied in written form in departmental manuals, or in formal pronouncements about how administrators intend to apply particular pieces of legislation. They may also take the form of general statements about how it is intended that powers and discretions will be exercised. Their provisions do not have legal force, in the sense of giving rise to legal rights and obligations, but they may lend legal legitimacy to administrative behaviour. They may also give rise to 'legitimate expectations' of a particular result or procedure, such that an administrator who is contemplating not giving effect to them may be obliged to give a hearing in relation to this issue to a person who might be adversely affected by the failure to apply the policy.

The Inquiry found a number of these rules hold up the Federal Information Principles (IPPs) and the National Privacy Principles (NPPs) as exemplars of good practice. Both sets of principles cover access and disclosure to confidential personal information. These principles are likely to be adopted in some form or other in the foreshadowed privacy legislation for Western Australia.

Western Australian Public Sector Code of Ethics

The *PSM Act* requires the Commissioner for Public Sector Standards to establish a code of ethics setting out the minimum standards of conduct and integrity for public sector bodies and employees. The current Western Australian Public Sector Code of Ethics came into effect on 1 March 2002. Compliance is mandatory and non-compliance can result in disciplinary action.

The term '***public sector body***' embraces departments, SES organisations, ministerial offices and non-SES organisations. While this might appear extensive, it does not cover a number of significant entities that are excluded from the term 'non-SES organisation'. The excluded entities are listed in Schedule 1 of the *PSM Act* (see Appendix 8) and include:

- elected officials (Members of Parliament and local government councillors);
- local government municipalities, shires, etc;
- police officers, universities, any court or tribunal established under a written law; and
- some corporatised bodies such as the port authorities, Western Power and the Water Corporation.

Note, however, that these organisations are covered by other legislation, which may contain provisions dealing with access and disclosure.[5]

The Code of Ethics includes requirements to:

- protect people's right to due process;
- refrain from using any circumstance or information connected to official duties for personal profit or gain;
- comply with an applicable code of conduct;
- protect privacy and confidentiality; and
- be conscientious and scrupulous in the performance of public duty.

It also requires the sharing of information 'wherever possible'. The Office of the Public Sector Standards Commissioner's website acknowledges the potential conflict between this requirement and the need to protect privacy and confidentiality and goes on to provide the following advice:

- Each request for information will need to be treated on its merits. This will be dependent upon a number of factors, like who has sought information, why it is being sought, the reason the information was collected in the first instance and whether the information is subject to confidentiality provisions through legislation/policy.
- Any decision to release or not release information needs to be carefully considered and documented. It is also suggested that the Office of the Freedom of Information Commissioner be consulted to assist in the decision making process.
- **Under no circumstances should information be released without appropriate authorisation** (emphasis added).

The Commissioner for Public Sector Standards advised by submission that s. 9 of the *PSM Act* requires all public sector employees to comply with the Code of Ethics and any agency-specific code of conduct. Further, 'an employee or member of a public sector body contravening the Code of Ethics commits a breach of discipline and may be subject to disciplinary measures'. The Commissioner for Public Sector Standards was not aware however, during her term of office, of receiving any information concerning a breach of a Public Sector Standard relating to unauthorised access and disclosure of confidential personal information.

According to legal advice quoted on the OPSSC website, the Code will generally take precedence over professional codes. This is because the Code is legislated, whereas professional codes are generally not.

[5] The *Local Government Act 1995*, for instance, has an offence of Improper Use of Information, which carries a penalty of a $10,000 fine or two years imprisonment.

It is not mandatory for agencies to have codes of conduct but if they do their employees must comply. The OPSSC website includes a Template Code of Conduct, developed specifically for government boards and committees, but which is based on the Code of Ethics and therefore provides a useful guide on what might be considered the ethical conduct in all public sector bodies.

The Template Code has a section on 'Record Keeping and Use of Information' which includes a sub-section on 'Use of Confidential Information'. After acknowledging that 'sometimes highly sensitive matters are discussed by boards', it goes on to say 'These may be discussed with only board members present and in strict confidence.' It then provides a boxed list of requirements:

> The Board will:
>
> - Ensure confidential records are subject to appropriate access procedures;
> - Respect confidential information and observe any restrictions agreed by the board (subject to *Freedom of Information Act* requirements);
> - Maintain confidentiality and not divulge information deemed confidential or sensitive. If members are uncertain they should seek direction from the board chairperson;
> - Not misuse information obtained in the course of board duties for direct or indirect gain, or to do harm to other people or the board;
> - Respect the privacy of individuals (p. 15).

The next sub-section, on 'Security of Information', is also relevant here. It acknowledges that the secretary or executive officer of the Board may be the person primarily responsible for the storage and handling of records, but adds that '… all board members have individual responsibility for any document, tape, disk or other record in their custody. Records should not be left in places where they may be seen by non-board members such as at home, an office or motor vehicle'. It then provides another boxed list of requirements:

> The Board will:
>
> - Ensure recorded information, in both paper and electronic form, under their control is kept in a secure place;
> - Be cautious about leaving board records on fax machines, photocopiers or computer screens;
> - Lock away sensitive documents rather than leave them lying on desks;
> - Avoid discussing board business in public places where there is a likelihood of being overheard;
> - Dispose of duplicate copies of records no longer required in accordance with archive procedures.

This template code provides sage advice that all public sector agencies would be well advised to adopt and incorporate into their own agency code of conduct.

Public Sector Recruitment, Selection and Appointment Standard

The Recruitment, Selection and Appointment Standard developed by the Public Sector Standards Commissioner requires *inter- alia* that the selection of staff be on the basis of a proper assessment of the candidate's skills, knowledge and abilities against the work-related requirements of the job. The Commissioner for Public Sector Standards in her submission to this Inquiry advised that her office would strongly encourage public sector agencies to:

- Ensure that arrangements for the selection, supervision or direct involvement of staff with access to information of a sensitive or confidential nature take into account and incorporate appropriate assessment processes to identify persons most suitable for this type of work; and
- Supervisors and managers provide proper induction and training for employees on the requirements of the Code of Ethics and the agency-specific codes of conduct that specify the confidentiality aspects of relevant positions.

Determining the suitability of staff to have access to confidential personal information is not an easy task and is generally beyond the scope of usual selection interviews. It involves an examination of the maturity of the individual together with an exploration of the person's background, interests and social involvements, etc. It is a task that requires a degree of specialisation and training and given the costs and intrusive nature, should be reserved for those positions where a risk assessment has determined that it is warranted. This issue of the vetting of staff is well covered in the Commonwealth Protective Security Manual and agencies are encouraged to consider its adoption.

As will be commented upon later in this report, agencies generally have a fairly well constructed and relevant induction program. The problem arises in that, often for reasons of operational exigency, new starters commence without benefit of the induction program. Even where induction does occur, the information imparted should not be on a once-only basis and there is a need for refresher training at appropriate intervals.

Treasurer's Instruction 825

A critical factor in the management of unauthorised access and disclosure is sound risk management. Under Treasurer's Instruction 825, which has the force of law by virtue of the *Financial Administration and Audit Act 1985*, Accountable Officers and Authorities in the Western Australian public sector are required to ensure there are procedures in place for the periodic assessment, identification and treatment of risks inherent in the operations of their departments or statutory authorities. They must also ensure 'suitable risk management policies and practices are developed' and an appropriate level of security is maintained over … public and other property of or under control of the department or statutory authority'. Unauthorised access and disclosure is an organisational risk that confronts each public sector agency, and needs to be mitigated against.

Fieldwork by the Inquiry indicated that few agencies considered unauthorised access and disclosure by staff or contractors as a risk inherent in their operations. This may be due to a failure to appreciate that confidential personal information is property. However, the fieldwork also found that two agencies,[6] both with significant holdings of confidential personal information, have been active in managing the risks of unauthorised access and disclosure. While in one case the activity has only been of recent date, in the other it dates back several years.

Treasurer's Instruction 825 has recently been amended to make particular reference to a requirement for agencies to take the risk of corruption and misconduct into account when determining the business risks to the agency. The definition of misconduct in the *Corruption and Crime Commission Act 2003* makes specific reference at s. 4(d)(iv) 'the misuse of information or material that the public officer has acquired in connection with his or her functions as a public officer, whether the misuse is for the benefit of the public officer or the benefit or detriment of another of another person'. In this way, agencies will in the future be required to consider corruption and misconduct, including the risk of unauthorised access and disclosure, in their risk management activities.

Instruction 825 needs to be further amended to include information held by an agency as a valuable asset that needs to be protected.

Premier's Circulars

Premier's Circulars focus on cross-government issues of strategic importance to the State and apply to all entities covered by the *PSM Act*, excluding those listed in Schedule 1 to the Act (See Appendix 8).

The following are the Premier's Circulars most relevant to the Inquiry:

PC NO 2005/02 ON CORRUPTION PREVENTION
The objectives of this Circular are to ensure that agencies consider the risk of corruption and misconduct as a component of their organisational risk and that they put plans in place to mitigate against such.

PC NO 2002/14 ON WEB SITE STANDARDS and the related **GUIDELINES FOR STATE GOVERNMENT WEB SITES**
The former is designed to 'provide guidance and a consistent approach for Western Australian Government agencies in establishing and maintaining current and future web sites'. It sets out 11 criteria which it states that WA government websites 'should aim to comply with', three of which are relevant to the Commission's Inquiry, namely that government agency on-line services should:

- take account of privacy concerns of the general public and implement strategies to ensure personal information is respected and protected;

[6] Department for Planning and Infrastructure (DPI) and Department of Community Development (DCD).

- ensure security is implemented and maintained in a manner consistent with best practices in IT security; and
- adhere to all relevant legal requirements.

The Circular does not state what privacy concerns it is referring to but the Guidelines for State Government Web Sites adopts the Information Privacy Principles published by the Office of the Federal Privacy Commissioner. The Principles appear in Appendix 2.

PC NO 2003/05 and the related **POLICY FRAMEWORK AND STANDARDS FOR INFORMATION SHARING BETWEEN GOVERNMENT AGENCIES**
The framework, which is now over two years old, is described as 'an interim arrangement until the development of broader information sharing legislation or privacy legislation is finalised'. It was introduced to 'facilitate sharing information on a structured basis, particularly confidential client information'. It sets out five high-level principles of information sharing that drive the Policy Framework and Standards, as well as four 'Enablers and Strategies for Implementation'.

The document states that the principles are intended to achieve an appropriate balance between competing interests of the community, agencies and individual clients. On that basis:

- Agencies must act within the limits of relevant legislation.
- Open and accountable processes and procedures are required for information sharing.
- Information sharing should be consistent with appropriate minimum privacy standards such as the National Privacy Principles.
- Procedures need to provide for the security of confidential information.
- Agencies sharing information do so within the context of information policies, procedures and practices, relevant legislation and privacy principles.

In this context it states that the reasons for collecting the information and how the information will be used or shared should be explained to clients at the time of collection. Although they do not directly apply to Western Australian Government agencies, the National Privacy Principles, for example, provide that information should only be used for the primary purpose of collection, and must not, with some exceptions, be used for a secondary purpose (a purpose other than for which it was collected).

Administrative Instructions

Administrative Instructions were issued under s. 19 of the *Public Service Act 1978*, which was replaced by the *Public Sector Management Act 1994*. A review of these Administrative Instructions at the time of the new Act's inception identified that, with the following nine exceptions, the Instructions were redundant:

102 Official Communications
601 Sick Leave

610 Effect on Grants of Leave and Period of Suspension on Salary and Leave Entitlements
706 Weekend Attendance at Work
707 Obligations of an Officer
711 Official Information
712 Fees, Rewards and Gratuities
726 Private Employment
728 Media and Public Communications

These nine Administrative Instructions have continued to remain in force under the transitional arrangements of the *PSM Act*. Of these, Administrative Instructions 711 and 728 are most relevant to this Inquiry.

Administrative Instruction 711, which took effect in 1989, prohibits an 'officer' from disclosing information except in the course of their official duties and with the express permission of his chief executive officer. Fieldwork by the inquiry indicated there was limited awareness of this Instruction. This Instruction covers disclosure of 'Official Information' and states:

> An officer shall not, except in the course of the officer's official duty and with the express permission of the chief executive officer:
>
> - Give to any person any information relating to the business of the Public Service or other Crown business that has been furnished to the officer or obtained by the officer in the course of his/her official duty as an officer; or
> - Disclose the contents of any official papers or documents that have been supplied to the officer or seen by the officer in the course of his/her official duty as an officer or otherwise; or
> - Disclose the contents of any Advertised Vacancy file that has been supplied to the officer or seen by the officer in the course of his/her official duty as an officer or otherwise.

The submission of the Director General of the Department of the Premier and Cabinet advised that Administrative Instruction 711 was criticised both in the WA Inc. Royal Commission and by the subsequent Commission on Government. The essential failing being the 'blanket effect' of these provisions being so broad as to make them inappropriate for achieving the objective of government. Support for this contention is to found in *Bennett v President, Human Rights and Equal Opportunities Commission* [2003] FCA 1433 and in a related legal opinion obtained by the Department of the Premier and Cabinet, which raises real doubt as to the validity of Administrative Instruction 711.

While good argument can be mounted to re-examine Administrative Instruction 711, and indeed all of the remaining Administrative Instructions, with a view to determining their continuing application, the Director General cautions against repealing them until such time as a firm replacement is promulgated. This is a result of concern that the ability to take action against a public officer would not be assured if reliance was placed solely on the high-level statements contained in the Western Australian Public Sector Code of Ethics supported by voluntary agency-specific codes of conduct. The Director

General advances the surest way to a consistent disciplinary approach would be through specifically targeted legislative provision. It is suggested that a suitably modified *PSM Act* could achieve this outcome, recognising however that it suffers from its limited application, particularly insofar as the large agencies exempted from its application (as listed in Schedule 1 – see Appendix 8) are concerned.

Oath or affirmation of secrecy

A number of agencies currently require the signing of written confidentiality agreements by employees, the staff of the Ombudsman being an example. Several agencies also require new employees to take an oath or affirmation before commencement – the WA Police, the Office of the Auditor General and the Corruption and Crime Commission being three such agencies. Furthermore, the Office of the Auditor General requires staff members to renew their declarations annually.

The oath taken by officers of this Commission under s. 183 of the *Corruption and Crime Commission Act 2003* has importance to this Inquiry, as it requires that:

> Before commencing duties as an officer of the Commission, the officer must take an oath or affirmation that, except in accordance with this Act, the officer will not disclose any information received by the officer under this Act.

The benefit of such a requirement can be evidenced in the 2002 finding of the Industrial Relations Commission (IRC)[7] concerning the summary dismissal of an officer of the former Anti-Corruption Commission (ACC) for misconduct. The misconduct involved an unauthorised disclosure of information that the officer was privy to by virtue of her position with the ACC. The IRC found that:

> … it was an express term of Ms …'s contract of employment that before commencing duties, she take an oath or affirmation to be administered by the Chairman of the ACC that, except in accordance with the Anti-Corruption Commission Act 1998, she will not divulge and information received by her under the Act. Ms … took that oath or affirmation. It is therefore apparent that if, as the ACC believes, Ms … had [made an unauthorised disclosure] she would have breached an express term of her contract and the ACC would be entirely justified in dismissing her.

Requiring all staff on commencement of employment in the public sector to take an oath or affirmation similar to that of the Corruption and Crime Commission would have positive benefits in highlighting the seriousness in which unauthorised disclosures are viewed, and clarifying the duty of officers to maintain secrecy, thereby overcoming one of the problems of s. 81 of the *Criminal Code*.

Pre-employment screening

Increasingly agencies are incorporating pre-employment screening in the recruitment and selection process. While this practice is endorsed, it should be noted that there are inherent limitations to criminal record screening. Screening is limited to court

[7] Application 1331/2001.

convictions and will not necessarily capture all of a person's relevant offence history. It was established during the course of this Inquiry that the National Police Clearance is based on the records held by each of the State and Territory police services together with those of the Australian Federal Police. What is missing from this check is the inclusion of records derived from prosecutions that are undertaken by agencies other than police and under legislation other than the respective criminal codes. As a consequence, a person convicted of dealing in unregistered vehicles under a fair trading Act, or such, may not have this revealed during a police clearance check. Similarly, prosecutions under various Acts such as those pertaining to the Department of Fisheries and the Department of Conservation and Land Management may also evade disclosure. Dependent upon the duties of the position being filled, these limitations may be of vital concern to the employing agency.

Other activity

Recent Governments have taken a number of steps to address the risks associated with increasing reliance on on-line services by agencies. In 2000, the former Department of Contract and Management Services was given the responsibility to implement a security management framework for all of government. More recently responsibility for information security assurance was vested in the Office of e-Government.

In 2003 the current Government released an e-Government Strategy which sets 2010 as the target date for full implementation of all key elements, including achieving secure and ethical management of personal information.

In the same year the Office of e-Government developed an information security management system (ISMS) methodology based on Australian and international standards including AS/NZS ISO/IEC 17799:2001 – Information Technology – Code of Practice for information security management. Adoption of this particular methodology, or an equivalent, based on the standards, is mandatory following State Cabinet's decision of 20 January 2003.

It is also developing a database to help agencies identify and record their information assets, conduct risk analysis and establish appropriate risk management strategies and treatments, and it offers a range of products and services including technical guides 'to assist in preparing for and responding to computer security incidents'. However, use of most of these services is not mandatory.

Another Office of e-Government initiative of relevance to this Inquiry is its current assessment of requirements for information classification, which is expected to result in the implementation of the information security classification scheme from the Commonwealth's Protective Security Manual.[8] This Commission endorses the adoption of the Commonwealth Protective Security Manual.

[8] GovSecure website (www.govsecure.wa.gov.au), 'Information Security Policies', as at 25/11/04.

The WA Government has a long-standing commitment to introduce privacy legislation. In 2004 it sought public comment on proposals covering a number of the issues over-lapping with the terms of reference of the Commission's Inquiry.

Specifically it put forward a framework that will:

- Apply 'to all public sector agencies, both State and local government, courts and tribunals (but only in respect of administrative functions, and not in respect of judicial functions) and private sector contractors performing work for government agencies or providing government services. In addition, health privacy laws should apply to the public and private sectors.'
- Include a set of Information Privacy Principles (IPPs), adapted from those in other jurisdictions, governing *inter alia* disclosure of personal information;
- Include a separate set of IPPs governing health information;
- Not create any enforceable rights except in accordance with the Act;
- Provide that subject to certain exemptions and exceptions, failure to comply with any one of the principles will be 'an interference with privacy';
- Include that the exemptions recognise the need to share vital information between government agencies;
- Give the proposed State Privacy and Information Commissioner the power to determine whether the public interest in adhering to a particular IPP is outweighed to a substantial degree by the public interest in an agency doing a particular act or engaging in a particular practice; and
- Include enforcement provisions similar to those contained in the *Information Privacy Act 2000* (Vic) to deal with 'serious or flagrant or repeated violations of information privacy principles or privacy codes of conduct'.

The inception of a privacy act and a related privacy commissioner is a progressive measure that is endorsed by this Commission.

Adequacy of the policy framework

The policy documents described in this section are a sample of the range and extent of policy directives and advice relating to the matters the subject of this Inquiry. This being so, it would be difficult to establish a case as to their inadequacy, at least in terms of volume.

It is apparent that there is a plethora of related policy instructions with Administrative Instruction 711 of 1989 among the more long-standing. It would appear that as new situations emerged a response in the form of a Premier's Circular, a Treasurer's Instruction, an Administrative Instruction, a new standard or code would be developed to remedy that which was ailing. This is to be expected. Over time, however, the confluence of these instructions is that they have created a most complex policy environment for agencies to adhere to.

Quantity is not of course a measure of compliance and indeed a number of public officers of considerable longevity in the public sector were not acquainted with Administrative Instruction 711 or many of the other policy documents referred to in this section of the report. This absence of specific knowledge of the documented requirements does not however mean that these persons were totally ignorant of the expectations of them. Rather, most were broadly aware of a requirement to maintain confidentiality of information, primarily in satisfaction of the specific expectations of their agency. Where good knowledge of these instructions was apparent, it appeared largely restricted to officers performing specific functions in a Head Office-type role.

While it is accepted that many of these policy documents have differing audiences and context, undoubtedly there would be benefits obtained in consolidating as many of these disparate but overlapping documents as possible.

Recommendations – Policy

It is recommended that existing policy in all its forms be reviewed by either the Department of the Premier and Cabinet, or the foreshadowed Privacy Commissioner, for the purposes of consolidation and to provide a sector-wide applicability. It is specifically recommended that:

- Policy be developed that covers all information held by government agencies, and which stipulates what information should be freely available to the public; is to be protected and not disclosed; and is to be protected and not disclosed except where it is in the public interest to do so. Efforts currently in progress towards the adoption of a Privacy Act for Western Australia and the appointment of a Privacy Commissioner will no doubt assist in this matter.
- Agencies review the level of authority that is required before releasing confidential personal information, with particular consideration to the amount of judgment and discretion allowed under agency disclosure policies.
- The Department of the Premier and Cabinet review existing policy directives, such as Administrative Instructions 711 and 728, to update such where necessary by amending or repealing, and to ensure that public officers are aware of the content of these directives and of their responsibilities under them.
- A public sector oath is introduced for administering to all public sector employees, which establishes the duty and reinforces the requirement to maintain confidentiality of information. The wording of s. 183 of the *Corruption and Crime Commission Act 2003* might provide a suitable model.
- Treasurer's Instruction 825 is amended to include information held by an agency as a valuable asset that needs to be protected.

Good Practice

Introduction

In assessing the practices of the sample agencies in terms of selection procedures, supervision arrangements and staff awareness, it is necessary to have some standards against which to make judgments. This area of public administration is well catered for in the form of guidelines, policy and report recommendations, etc. As the following examples serve to illustrate, agencies that want to update their policies and procedures, and are seeking good practice initiatives to base them upon, have quite a selection to choose from. Although this Inquiry has largely steered away from information technology solutions, it has not been possible to do this entirely, and some of the following comments and recommendations reflect such.

Standards

Significant broad guidance can be taken from published standards. The Organisation of Economic Cooperation and Development (OECD) *Guidelines for the Security of Information Systems and Networks (2002) – Towards a Culture of Security* identify, among other things, nine principles of information security. Those principles deal with the issues of accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, reassessment and democracy.

Further broad guidance can be taken from a number of publications of Standards Australia relating to Risk Management and a Code of Practice for information security management. Standards Australia & New Zealand Standards, 2004, AS/NZS 4360:2004 Risk Management (the Risk Management Standard) and Standards Australia & New Zealand Standards, 2004, HB: 4360:2004 Risk Management Guidelines – Companion to AS/NZS 4360:2004 Risk Management (the Risk Management Guidelines) provides a generic guide for managing risk that may be applied to a wide range of activities, decisions or operations of any public, private or community enterprise, group or individual.

More specifically, Standards Australia & New Zealand Standards, 2001, AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management (the Standard Code of Practice) gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation.

The Standard Code of Practice is intended to provide a common basis for developing organisational security standards and effective security management practice and to provide confidence in inter-organisational dealings.

In addition, guidance can be taken from a wide range of sources, including:

- Information and privacy review bodies in Australia and overseas;
- Corruption and integrity bodies in Australia and overseas; and
- Other independent review bodies in Australia and overseas.

Although some valuable broad guidance can be taken from the OECD Guidelines, the Risk Management Standard, the Risk Management Guidelines, the Standard Code of Practice and the various other sources described above, it is considered that more jurisdiction-specific guidance is appropriate for the purpose of this Inquiry's terms of reference. In particular, it is considered best to identify well-established practice in the Australian public sector that is based upon:

- relevant legislative framework (privacy or data/information protection legislation);
- consolidated and centrally coordinated government policy direction; and
- ongoing independent review (eg. Privacy Commissioner, Auditor General, Independent Commission Against Corruption or Crime and Misconduct Commission).

Government policy direction

At present, there is not a consolidated and centrally coordinated government policy direction in relation to privacy and the risk management of the security of personal information. However, there are a number of policies, instructions, circulars and guidelines issued by a number of agencies that together provide high-level policy direction by the Government. Those documents include, but are not necessarily limited to, the following:

- Accountability in the Western Australian Public Sector, 1998 – Public Sector Management Office, Department of the Premier and Cabinet.
- Fraud Prevention in the Western Australian Public Sector, 1999 – Public Sector Management Office, Department of the Premier and Cabinet.
- Guidelines for Managing Risk in the Western Australian Public Sector, 1999 – Public Sector Management Office, Department of the Premier and Cabinet.
- Corporate Governance Guidelines for Western Australian Public Sector CEOs, 1999 – Public Sector Management Office, Department of the Premier and Cabinet.
- Managing, Monitoring, Audit, Review and Evaluation Activities in WA Public Sector Agencies, 1995 – Public Sector Management Office, Department of the Premier and Cabinet.
- Various best practice publications of the State Records Commission, for records management services, including minimum standards for Record Keeping Plans of agencies.
- Premier's Circular No. 2003/05 – Policy Framework and Standards for Information Sharing between Government Agencies.

Privacy legislation

At present, Western Australia does not have privacy legislation. In 2001, the current Government took a policy to the 2001 State Election that it will:

- introduce privacy laws to protect personal information held by the State public sector;
- monitor the impact of new technologies on Western Australia's privacy rights; and
- encourage good privacy practices in the private sector.

In May 2003, the Attorney General issued a discussion paper and a policy research paper for privacy legislation in Western Australia. A Privacy Working Group, working under the Attorney General, received submissions, and a response to those papers has been given for the drafting of legislation. It appears likely that Western Australia will have privacy legislation before the end of 2005. This development is welcomed, as it is hoped that this body will provide the central coordinating role that is currently missing.

Privacy principles

Whether agencies have privacy policies and procedures in place or are interested in developing such in the future, the Commission is of the view that any undertaking by a State or Local Government agency should address the issue of information security by adopting the Information Privacy Principles (IPPs) and the National Privacy Principles (the NPPs) described in the *Privacy Act 1988* (Commonwealth) as a minimum benchmark from which to work.

The Commission is of the view that the IPPs and NPPs represent part of the standards that have now become widely expected in the community and by public sector administrators in dealing with confidential personal information held by public sector agencies.

The discussion paper and a policy research paper for privacy legislation in Western Australia issued by the WA Attorney General in May 2003 indicates that, at that stage, much of the Victorian privacy model may be adopted. The Victorian model appears to have been developed to a large extent from the Federal model and the NSW model.

Given that, it appears reasonable to proceed in a manner that is 'legislation ready' so that agencies will develop a privacy compliance culture before being obliged by law to comply with the anticipated introduction of privacy legislation in WA.

The 11 Information Privacy Principles established under the Commonwealth *Privacy Act 1988* have become the *de facto* standard in Western Australia, by virtue of various WA Government policies on information management. In relation to access and disclosure of confidential personal information, the Principles incorporate the following provisions:

- Responsibility of the record-keeper to protect information against unauthorised access, use, modification, or disclosure;

- Responsibility of the record-keeper to prevent unauthorised use or disclosure by authorised third parties;
- The subject's entitlement to access the information;
- Use of the information only for a relevant purpose;
- Permitted use of the information for other prescribed purposes, including;
    - prevention of personal harm;
    - under legal authority;
    - for law enforcement or protection of public revenue;
    - with the consent of the subject;
- Prohibition of disclosure except:
    - with consent of the subject;
    - prevention of personal harm;
    - under legal authority; and
    - for law enforcement or protection of public revenue.

Risk assessment – Information security

The Commonwealth Protective Security Manual 2000 is a comprehensive guide that has been in place for a number of years and has already been the subject of review and refinements. The Manual deals in some detail with:

- Protective Security Policy
- Guidelines on Managing Security Risk
- Information Security
- Personnel Security
- Physical Security
- Security Framework for Competitive Tendering and Contracting
- Guidelines on Security Incidents and Investigations
- Security Guidelines on Home-base Work

Although much can be drawn from the entirety of the Manual, of most relevance to the terms of reference of the Inquiry is Part C. Part C deals with Information Security and describes eight principles of effective information security practice as follows:

1. Anyone with access to an agency's information must be made aware of the agency's expectations about the use and care of that information.
2. Anyone, including a contractor, who has access to an agency's information, must handle all that information with care.

3. Information held by agencies, including that held on information systems and networks, must only be used in accordance with government policy and agency direction.
4. The availability of information should be limited to those who need to use or access the information to do their work.
5. Agencies must ensure that all the information for which they are responsible is secured appropriately.
6. All Commonwealth information systems, whether they are paper-based information systems or information technology and telecommunication (IT &T) systems, used for processing, storage or transmission of official information require some protection to ensure the system's integrity and reliability.
7. Where the compromise of official information could cause harm to the nation, the public interest, the Government or other entities or individuals, agencies must consider giving the information a security classification.
8. Once information has been security classified, agencies must observe the minimum procedural requirements for the use, storage, transmission and disposal of security classified information.

The Commission believes that the above principles can be readily adapted to suit the circumstances in this State.

Summary of good practice models

Unlike the current situation in Western Australia, the Commonwealth has a well-established privacy regime formed substantially around the *Privacy Act 1988*, together with consolidated and centrally coordinated government policy direction in relation to risk management across government that specifically addresses issues relating to information security. That policy direction is enshrined in the Commonwealth Protective Security Manual, 2000 issued by the Commonwealth Attorney General's Department, and well-established and comprehensive independent review process administered by the Australian National Audit Office (ANAO).

The Independent Commission Against Corruption (NSW) and Crime and Misconduct Commission (Qld) have produced guidelines and checklists that were prepared following inquiries conducted by each agency and/or based on reports of commissions of inquiry that preceded the establishment of each of these commissions. The lessons learnt from those experiences are also reflected in the practices recommended by the ANAO and incorporated in the Commonwealth Protective Security Manual. These documents are commended as providing suitable good practice models for adoption by Western Australian state government agencies.

Opinions

At present Western Australian public sector agencies have not taken advantage of the good practice models provided by the Commonwealth in a coordinated and structured way. As a result, agencies are expected to comply with an array of legislation and policy without adequate guidance on how this should be achieved.

There is benefit to be obtained by agencies using the good practice examples identified in this report for application to their circumstances. There would be much to gain from adopting the Commonwealth Protective Security Manual in its entirety.

Recommendation – Commonwealth Protective Security Manual

It is recommended that all agencies in the public sector adopt the Commonwealth Protective Security Manual.

Recommendation – Review and development of systems in line with ISO 17799

It is recommended that when reviewing existing and developing new security policies, procedures and systems, agencies do so in line with Organisational Standards Australia & New Zealand Standards, 2001, AS/NZS ISO/IEC 17799:2001 Information technology – Code of practice for information security management (the Standard Code of Practice).

Fieldwork Summary Report

Overview

The fieldwork component of this Inquiry aimed to address each term of reference by examination of legislation, policy, and procedure at the following six agencies:

- City of Melville
- City of Rockingham
- Department for Community Development (DCD)
- Department of Justice (DOJ)
- Department for Planning and Infrastructure (DPI)
- Insurance Commission of Western Australia (ICWA)

The agencies were selected on the basis of perceived risk, public interest, and to capture a range of information types and information practices.

Agency policies and practices were assessed against legislative requirements and identified good practice. This included good practice in relation to:

- Definition and classification of confidential and public information;
- Legislative and policy environment;
- Access to confidential personal information;
- Authorised disclosure of confidential personal information;
- Management of known instances of unauthorised access and disclosure;
- Selection and supervision of staff with access to confidential personal information; and
- Staff awareness of responsibilities.

Definition and classification of personal and public information

What was expected:

- Each agency to have clearly defined what information is confidential and what is available to the public.
- Confidential personal information to be further classified into security levels.
- Each agency to have a record of what confidential personal information it holds and where it holds it.

Definition and classification of confidential personal information

The agencies reviewed could more clearly define what of the information they hold is confidential information, and what is publicly available. This would make clear to employees which information is to be protected and which can be disclosed. Agencies risk unauthorised disclosure of confidential personal information when the status of information is unclear and employees are required to make decisions on a case-by-case basis.

As per the Commonwealth Protective Security Manual, most information held by public sector agencies will be adequately protected by an X-in-confidence classification. Examples of X-in-confidence include staff-in-confidence, security-in-confidence, commercial-in-confidence, and audit-in-confidence. Access to X-in-confidence information should be on a need-to-know basis and disclosure should only be in accordance with legislative and administrative requirements. Although the majority of information held by public sector agencies is unlikely to require a higher security classification, agencies should assess the risk of unauthorised access and disclosure of all information and classify it accordingly. The agencies reviewed utilised very limited security classification. This largely involved classifying information into functional areas. None of the agencies reviewed had security classified the confidential personal information that they hold on the basis of a documented risk assessment.

Table 1: Security classification scheme (Commonwealth Protective Security Manual, 2000).

Public domain: Information authorised for unlimited public access and circulation.	
Unclassified: Official information that does not need to be security labelled or classified, but requires authorisation to release.	
Security classified: Information for which unauthorised disclosure or misuse may have adverse consequences.	
National Security Information	**Non-National Security Information**
Restricted Confidential Secret Top Secret	X-in-confidence Protected Highly Protected

DPI was the only agency that clearly defined what was confidential information and what was publicly available. The DPI Freedom of Information Statement includes lists of information under these categories. DPI's Information Security Policy, which the Inquiry was advised was endorsed by the agency's executive level Information Management Committee at a meeting held during the Inquiry's fieldwork phase, calls for information to be clearly labelled with its security classification. The Policy expressly recognises the four categories set out in Table 1 while also noting that the agency is unlikely 'in all but the rarest of circumstances' to handle National Security Information. In relation to Non-National Security Information it also expressly refers to the three sub-categories referred to in Table 1. It goes on to call for all information assets, except 'Unclassified' materials, to be clearly labelled with their classification and that 'Information labelling shall apply to both physical and electronic media; the

mechanism for labelling being determined as appropriate to the specific media characteristics.'

Of the other agencies reviewed:

- DCD uses some information definitions (such as 'official information'), but has no definitions or classifications of 'confidential information'.
- DOJ refers to 'personal information' in its Freedom of Information Statement, but does not classify information according to confidentiality or security. Different levels of access may be applied by restricting access to certain types of information, but this is done on a need-to-know basis, rather than using a security classification scheme.
- ICWA makes reference to the availability of categories of information listed in the Freedom of Information Statement, but the actual confidentiality of this information is not clear.
- The two local government authorities – the City of Melville and the City of Rockingham – have not clearly defined what information is to be classified as confidential.

Register of confidential personal information

Each of the agencies, except DPI, were able to supply a comprehensive record of what confidential personal information is maintained on databases by the agency. DPI has acknowledged that not all database systems held by the agency are known at a corporate level, but has advised that they are currently addressing this. The list of databases supplied by DCD was notably more comprehensive than the list provided in the Freedom of Information statement. DOJ has reported that it intends to adopt the Office of e-Government's recommended data security classification system.

Table 1: Definition and classification of confidential personal information at the fieldwork agencies.

	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Clear definitions of what is confidential and what is publicly available.			✓			
Security classifications.			✓			
Comprehensive record of what is held.	✓	✓		✓	✓	✓

Legislative and policy environment

What was expected:

- Each agency to have a legislative and policy framework that governs the protection and access to personal information it holds.
- Each agency to have a clearly defined administrative authority for the protection and access to personal information.

Legislative and policy framework

Legislation

In addition to the global state public sector legislation governing the management of confidential personal information, DCD and ICWA have agency-specific legislative provisions regarding the treatment of confidential personal information. For DCD, this includes clauses in the *Adoption Act 1994*, the *Children's Court of Western AustraliaAct 1988*, and DCD's establishment Act, the *Community Services Act 1972*. For example, the *Adoption Act* prohibits the recording, use, or disclosure of adoption information and the *Children's Court Act* restricts the disclosure of Court decisions and orders. Both Acts impose penalties of $10,000 fine and/or 12 months imprisonment.

The two legislative instruments governing confidentiality at ICWA are the *Insurance Commission of Western Australia Act 1986* (*ICWA Act*) and *Motor Vehicle (Third Party Insurance) Act 1943*. Section 42 of the *ICWA Act* makes it an offence to make a record of or divulge ICWA official information and provides for a penalty of $2,500. The *ICWA Act* also states that the Act does not entitle the Minister to information that discloses or enables identification of any person who is or has been a customer of the Commission (s. 10B). This does not, however, apply to information covered under s. 25 of the *Motor Vehicle (Third Party Insurance) Act*, which may be provided to the Minister upon reasonable request.

The Department of Justice and DPI do not have agency-specific legislation governing the treatment of confidential personal information. However, there is provision in the Prisons Regulations 1982 for dealing with appropriate use of information by prison officers. This would be relevant to those staff of DOJ covered under the *Prisons Act 1981*.

The two local government authorities are bound by the *Local Government Act 1995* (*LG Act*), which prohibits 'improper use of any information' acquired by council members, committee members and council employees. The *LG Act* also requires all local governments to have a code of conduct but there is a general view that the codes are not legally enforceable.

Policy

Each of the sample state government agencies has a comprehensive policy framework, including the agency Code of Conduct. In the case of DCD this is spread across a range of policy documents, instructions and manuals, without an apparent central, summary, or overarching policy. This has the potential to make the interpretation and application

of departmental policies difficult and inconsistent across staff and contexts. This is particularly the case at DCD, where previous complaints to this Commission have made specific reference to the range and complexity of policies and instructions regarding confidentiality of client information. ICWA, DOJ and DPI appear to have principal policy documents dealing with confidential personal information. At ICWA, the main policy document is the Information Systems Security policy, which contains four key principles and a number of guidelines for accessing and managing information. At DOJ, there is an overarching Confidentiality and Information Privacy Policy, while at DPI, the principal documents are the Information Security Policy, and Client and Employee Information Policy.

The Inquiry did not identify any policies dealing with confidential personal information at the two local government authorities other than the Codes of Conduct.

Administrative framework
Three of the state government agencies reviewed – ICWA, DOJ and DPI – have allocated data custodians from within operational line management for each database or system that contains confidential personal information. The custodians have a number of responsibilities, including authorising user access. In addition to the data custodians, DOJ also has a Custodial Applications Manager based at head office, and branch office-based System Administrators.

DPI has allocated a number of roles and responsibilities for information security, which are oversighted at corporate executive level by an Information Management Committee.

For DCD's main client database, the Client and Community Services Systems (CCSS), access is recommended by work unit managers, however, the internal User Manager CCSS has ultimate responsibility for authorising this access. For other DCD databases there are custodians within operational line management.

At the two local government authorities, the administrative framework appears to rest with information technology management. At both authorities, the in-house Information Technology Manager is responsible for managing information access and security.

Access to personal information

What was expected:

- Each agency to have assessed the risk of unauthorised access and disclosure of personal information.
- Access to be controlled in accordance with general information privacy principles and assessed risk.
- The physical and electronic security environment supports access controls.
- The agency to monitor access, investigate suspected unauthorised access, and report access compliance to senior management.

Risk assessment

With the exception of DCD, the agencies examined do not conduct a comprehensive and documented assessment of the risks of unauthorised access and disclosure of confidential personal information. In 2003, DCD commissioned penetration testing of its network. This resulted in the identification of risks to network security, including unauthorised access to confidential client information.

ICWA has advised that it is planning a risk assessment project that will result in a security classification for information assets.

DPI has advised that risk assessments at the level of individual system owners will be the first step taken to implement its new information security policy.

DOJ has advised that it is currently represented in an Inter-Agency Information Sharing Group, which has recommended to its parent group, the Information Security Management Group, the adoption of the Commonwealth Protective Security Manual. The objectives are to:

- develop an Information Systems Classification scheme to be used across all Government agencies;
- identify base level security controls required for each classification level; and
- establish guidelines to facilitate the sharing of information across Government agencies.

DOJ reports that it has the Intrusion Detection and Prevention Systems which detects abnormal traffic to its e-business environment. The Department is in the process of establishing ongoing system assurance such as penetration testing, vulnerability assessments and application security reviews.

Access controls

Four of the six agencies reviewed have advised that they have formally adopted the Information Privacy Principles[9] established under the *Commonwealth Privacy Act 1988*.

A summary of database access controls at each of the agencies reviewed is shown in Table 3.

Table 3: Summary of access controls at fieldwork agencies.

Access Control	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Management approval of user access rights.	✓	✓	✓	✓	✓	✓
Logon ids.	✓	✓	✓	✓	✓	✓
Individual passwords.	✓	✓	✓	✓	✓	✓
'Strong' passwords.	✓	✓		✓		
Periodic or incident driven review of access rights.	✓	✓	✓			
Restricted access.	✓	✓	✓		✓	✓
Timed computer lockdown	✓	✓	✓	✓		

[9] ICWA, City of Rockingham, City of Melville and DPI.

Consistent with the Information Privacy Principles, the agencies reviewed generally restrict access to information on a need-to-know basis. The City of Rockingham, for example, has advised that different officers (such as Community Services Officers, Engineering Officers, and Planning Officers) have different access based on their work requirements.

DOJ and DPI have implemented additional *ad hoc* security controls over certain sensitive databases.

Monitoring, investigating, and reporting

Each of the agencies reviewed protects the integrity of the personal information they hold in electronic databases by electronically recording (logging) all data changes.[10] Read-only access to personal information, however, is only logged by DOJ for the Total Offender Management System (TOMS) database, and by DPI for the TRELIS database (Transport Executive and Licensing Information System).

Both DPI and DOJ use the logs to investigate reported breaches. However, the logs are not routinely monitored to identify possible unauthorised access to TRELIS and TOMS information respectively.

Table 4: Monitoring, investigating, and reporting at fieldwork agencies.

Access Control	DCD (CCSS)	DOJ (TOMS)	DPI (TRELIS)	ICWA	City of Melville	City of Rockingham
Data changes are logged.	✓	✓	✓	✓	✓	✓
Read-only access is logged.		✓	✓			
Logs are routinely monitored.						
Logs are used to investigate reported breaches.		✓	✓			
Access compliance is regularly reported to senior management.						

Authorised disclosure of personal information

What was expected:

- Each agency to have formal policies and procedures for authorising the disclosure of personal information.
- The disclosure of personal information to be made only under the authority of that framework.

[10] In DCD not *all* screens can be logged for data changes.

Policy and procedures for authorised disclosures

The Commonwealth Information Privacy Principles state that the disclosure of confidential personal information must be:

- where reasonable, with consent of the subject;
- only for a relevant purpose, except where it is,
  - to prevent personal harm,
  - made under legal authority,
  - for law enforcement or protection of public revenue; and
- recorded.

Each of the agencies reviewed has formal procedures for authorising the disclosure of confidential personal information,[11] and these generally incorporate the above requirements. ICWA's Information Statement and Privacy Guidelines, for example, state that where the Insurance Commission wishes to use or disclose personal information it will use all reasonable endeavours to obtain the consent of the person concerned, other than in exceptional circumstances such as where:

- it is necessary to protect any person and/or the Insurance Commission's rights or property;
- the use is authorised by law or is reasonably necessary to enforce the law;
- personal information may also be exchanged within the Insurance Commission or its agents for claims management purposes and/or investigations into claims; and
- the use and disclosure of personal information will at all times comply with the *FOI Act* and *State Records Act*.

Authorised disclosures at the agencies examined can involve the disclosure of confidential personal information to:

- Legal counsel;
- Medical practitioners;
- Private investigators;
- Ministers of the Crown;
- Police officers; and
- Other WA State, other State and Commonwealth government agencies.

Disclosure policies and procedures vary in prescription and complexity. ICWA, for example, prohibits the disclosure of official information except in the course of official duties and with the express permission of the Chief Executive Officer. This is consistent with Administrative Instruction 711.

[11] This is in addition to processes established under the *Freedom of Information Act 1992*.

Other agencies have more complex rules and allow officers to exercise greater discretion to act. The DCD Director General's Instruction 16, for example, covers the release of information under a range of circumstances. This includes the release of information from client records to third parties, which is permitted only 'in order to protect or benefit a particular child or children, or as part of a referral for an individual or family for assessment or treatment'. Such information may only be released with the knowledge and permission of the person concerned, unless release without consent is considered by the District Manager to be 'clearly necessary for the purpose of advancing the best interests of a child or children'. Instruction 16 is, however, only one of a number of policies and legislative clauses relating to the disclosure of confidential personal information.

The agencies reviewed generally did not keep a centralised record of authorised disclosures other than information released under the *Freedom of Information Act*.[12]

Inter-agency standing agreements to share information

Each agency shares confidential personal information where it is legally required to do so. The legal requirements may arise under either Commonwealth or State legislation, with the latter including by-laws enacted by local government authorities under the *Local Government Act*. In addition, agencies may have formal standing agreements to share confidential personal information either on an *ad hoc* basis or via on-line access to the agency's database. Refer to Appendix 3 for a list of information sharing arrangements at DPI.

Notable aspects of the information sharing arrangements at the fieldwork agencies include:

- the use of nominated officers to facilitate the exchange of information (ICWA, DCD, WAPS),
- interagency memorandums of understanding covering sharing and transferring of information between agencies, (DOJ with WAPS)
- unequal provisions for protecting confidentiality, where the provisions are less rigorous for the exchange of information between state government agencies.

A positive outcome of this Inquiry is that the City of Rockingham has advised that it is contacting all of the external organisations that have access to City confidential personal information by way of service agreements in order to:

- identify the appropriateness of their policies regarding confidential personal information; and
- develop appropriate policies where required.

[12] At DCD the Family Information Records Bureau records authorised disclosures.

Management of known instances of unauthorised access and disclosure

What was expected?

- Each agency to have formal procedures for managing suspected unauthorised disclosure of personal information.
- Each agency to maintain records of instances of unauthorised disclosure and of their reporting to senior management.

Procedures for managing suspected unauthorised access and disclosure

Each of the four state government agencies have formal procedures for managing identified cases of unauthorised access and disclosure of confidential personal information. These are described in brief in the following paragraphs. Neither of the two local government authorities have formal procedures in place, however they both require staff to report known or suspected breaches.

ICWA's Information Systems Security Policy contains a section on Security Incident Management, which provides guidance on the proper response to the misuse of IT resources from within or outside the Insurance Commission. This includes a notification process, requirements to document processes, evidence gathering, and incident reporting.

DCD's Discipline Procedures in their Best Practice Manual (s.1.4.8) provide a formalised process to investigate suspected breaches of discipline (including the unauthorised access and disclosure of confidential personal information) and, where necessary, initiate disciplinary action. The policy refers to s. 80–92 of the *PSM Act* and associated regulations for investigative procedures. Responsibility for discipline procedures rests with the line manager, who is required to consult with the relevant Executive Director (for levels 1–7) or Director General (for Levels 8 and above).

DPI have disciplinary procedures covering breaches of discipline by in-house staff as well as incident management procedures. These include a requirement for staff to report known or suspected breaches. Under their new Information Security Policy, incidents are required to be logged and reported to the Information Management Committee.

Reported or suspected breaches at DOJ are investigated by their Internal Investigations Unit where the breach has occurred in the prisons or community-based services programs. Breaches in all other program areas are managed by the Director General's office. Investigations are reported to the Investigation Review Committee and the outcomes are referred to the Discipline Review Committee. The Director General signs off on all investigation reports.

Both local government authorities and ICWA advised that there were no unauthorised disclosures during the period January 2004–present.

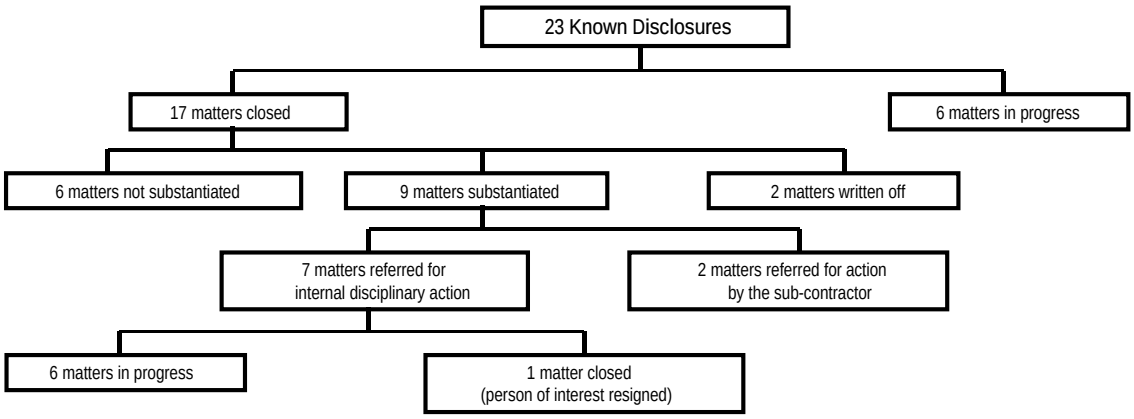
Investigation outcomes

Examination of known instances of unauthorised access and disclosure in DOJ, DCD and DPI[13] suggests that agencies may be experiencing difficulty in establishing offences under the *Criminal Code* and/or misconduct under the *Corruption and Crime Commission Act 2003* or in establishing a breach of discipline under the *Public Sector Management Act 1994*. This is due to a number of reasons, including the inability to establish:

- whether the person of interest accessed a record due to a lack of electronic logging of read-only accessed;
- whether the person of interest accessed a record due to agency operational practices that enable multiple persons to access or sight records under one user identification;
- that a record was accessed for other than official duties; and
- that the information contained in a record was disclosed to a third party.

The following figure illustrates one agency's progress in managing known instances of unauthorised disclosures identified since January 2004.

Figure 1: Management of known instances of unauthorised disclosures at one fieldwork agency.



Public Sector Investigation Unit – Western Australia Police Service

The submission of the Public Sector Management Unit (PSIU) included that there were a number of impediments to investigations by the PSIU, relating to misuse of computers by employees of various government agencies. It was their belief that problems relating to unauthorised access and disclosure were contributed to by:

- a lack of adequate training of public officers. It was felt that there is a minimal awareness of the rules and regulations applying to the use and access of computer information following initial training;

[13] This includes cases in the CCC database and cases that have occurred at the fieldwork agencies since January 2004.

- a lack of written confirmation of acknowledgement by employees of obligations and regulations involved with use of agency computers and access to various databases;
- a lack of written conformation of acknowledgement by employer as to making employees aware of obligations and regulations involved with use of agency computers and access to various databases;
- the practice in some agencies of staff sharing passwords; and
- a lack of awareness of the seriousness of breaching policy and guidelines associated with computer use.

The submission also advised of the belief that agencies generally lacked a process or ability to conduct internal audits of an employee's use of computers and databases as there was no means of recording the individual's computer use – such as does occur in the WA Police.

The experience of the PSIU was that these factors in combination served to make it difficult to detect unauthorised use and, where such misuse was suspected, difficult to gain sufficient evidence to secure a conviction.

Selection and supervision of staff with access to confidential personal information

What was expected:

- Each agency to conduct pre-employment screening commensurate with each new employee's access to personal information.
- Screening of existing employees is up-dated according to assessed risk.
- Each agency has supervision procedures for ensuring that staff only access information that is relevant to their work.
- Screening and supervision arrangements are in place for contractors with access to personal information.

Pre-employment screening is a method for assessing the integrity of potential employees and contractors who will have access to confidential personal information as part of their duties. Criminal records checks, in particular, can identify potential employees who may be at greater risk of inappropriately accessing and disclosing confidential personal information.

The agencies reviewed varied in their approach to pre-employment screening. DCD and DOJ both conduct criminal records checks for all new staff. DCD also conduct additional screening using departmental records to identify whether a potential employee has been believed responsible for harming children, and DOJ screens department records for any new employee who will have contact with children. Three agencies – DPI, City of Melville, and City of Rockingham – each advised that they conduct criminal records screening for new staff on a case-by-case basis, based on position requirements. At DPI, this has recently included obtaining a national police clearance for all new licensing staff.

To confirm these practices, the Inquiry Team examined the personnel records for a random sample of 32 staff at the two local government authorities. Each of the staff members examined had access to confidential information regarding ratepayers and 10 of the staff members had system-wide access, including the ability to alter and delete ratepayer information. Examination of the personnel files indicated that:

- none of the employees were required to provide proof of identify upon employment;
- none of the employees were screened for previous criminal records (although two employees provided a copy of a WA Police clearance as part of the position application); and
- none of the employees were required to sign confidentiality agreements, with the exception of three senior officers who had confidentiality clauses included in their employment contracts.

The Insurance Commission of Western Australia does not conduct criminal records screening for new staff and relies on self-disclosure of criminal records as part of the employment application.

None of the agencies examined advised that they regularly update criminal records screening for existing staff. DPI has advised that they conduct cyclical updates 'where appropriate' and update police clearances for existing staff who require different levels of access (for example, in the case of staff promotion). This Inquiry has not, however, found evidence to support this practice. DOJ has also advised that it has a draft self-disclosure policy for existing employees.

Table 5: Summary of arrangements for screening and supervising staff and contractors with access to confidential personal information.

	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Pre-employment screening.	Crimtrak screening for all new staff. Additional departmental records screening to identify persons believed responsible for harming children.	Crimtrak screening for all staff. Additional screening where position involves contact with children.	Screening is conducted at the discretion of the business unit. All JDFs in the licencing area state that a national police clearance is required (since 2004).	Self-disclosure of criminal records.	Case-by-case based on position requirements.	Case-by-case based on position requirements.
Staff confidentiality agreements.	Yes		Yes (since 2004)	Yes	Relevant policy exists.	Case-by-case based on position requirements.
Screening updates for existing staff.	Policy exists.	Draft self-disclosure policy. Employees in high risk positions screened every two years.	Clearances are updated or renewed when access to sensitive information is required. Cyclical updates are conducted on all staff where appropriate.			

	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Supervision arrangements for staff.	Yes	Ad hoc arrangements.				
Contractor screening.		Yes	Yes			
Contractor confidentiality agreements.	Confidentiality is covered in the KAZ information services contract.	Yes	Yes			
Supervision arrangements for contractors.			DPI retains the rights to inspect staff selection processes and premises. Contract remedies for breaches.			

Staff and contractor awareness of responsibilities

What was expected:

- Each agency to have clearly defined staff and contractors' responsibilities to protect personal information.
- Each agency to have strategies to ensure that staff and contractors are aware of their responsibilities to protect personal information.

Agencies use a range of tools to ensure that staff and contractors are aware of their responsibilities to protect confidential personal information. All of the agencies reviewed advised that they include confidentiality of information in their staff induction training and most agencies provide access to relevant agency policies on the agency intranet.

Table 6: Summary of agencies' strategies to inform staff of their responsibilities regarding confidential personal information.

	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Strategies to inform staff.	Staff induction material.	Staff Induction Manual Pre-employment checklist DoJ On-line responsibility statement.	In-house bulletins Policies placed on the Intranet.	HR Induction Checklist Senior management contract of employment. Staff emails (provided).	Email and intranet notices. Code of Conduct and other relevant standards are on the intranet.	Email and intranet notices. Code of Conduct and other relevant standards are on the intranet.

	DCD	DOJ	DPI	ICWA	City of Melville	City of Rockingham
Training.	Adoption Services Training Course DCDNet Induction package.	JustNet Induction program.	Mandatory and other training, including induction, PID, TRELIS, on-line agent training, licensing staff training, and mandatory 'values' workshops.	Induction Training. Security Overview Training Program.	Induction training.	Induction training.
Information and training for contractor staff.						

Examination of personnel files at the City of Rockingham and the City of Melville was undertaken to confirm these practices, with the following results:

- Of the 16 personnel files reviewed at the City of Rockingham, only seven indicated that employees had participated in an induction process. Six of those involved the completion of an induction checklist that included items relating to confidentiality of information and, more recently, one employee had attended an induction workshop. None of the personnel files reviewed indicated attendance at relevant refresher training.
- Of the 16 personnel files reviewed at the City of Melville, only five indicated that employees had participated in an induction that included items marked on an induction checklist relating to confidentiality of information. None of the personnel files reviewed indicated attendance at relevant refresher training.

Opinions and issues

The following issues were identified in the course of the fieldwork:

- Agencies have not clearly defined which information is confidential and which is publicly available – and they need to do so.
- There is very limited security classification of information and the adoption of the Commonwealth Protective Security Manual is recommended for this purpose.
- Only one agency has assessed the risk of unauthorised access and disclosure of confidential information. Such risk assessment should form a component of the risk management activities undertaken in accordance with the requirements of Treasurer's Instruction 825.
- Only two agencies record access to confidential personal information, and none of the agencies actively monitor these logs to identify possible unauthorised access.

- Agency policies for the authorised disclosure of personal information generally comply with the Commonwealth Information Privacy Principles.
- The policy frameworks at some agencies are complex, with the result that application of agency policies to individual decisions may be overly difficult, leading to inconsistent application of disclosure rules.
- Agencies in general do not review the level of authority that is required before releasing confidential personal information, with little or no consideration to the amount of judgment and discretion allowed under agency disclosure policies.
- Each of the four state government agencies have formal procedures for managing identified cases of unauthorised access and disclosure of confidential personal information. However, none of these acknowledge unauthorised access and disclosure as being misconduct pursuant to the *CCC Act* or identify when cases should be reported to the Corruption and Crime Commission.
- It may be difficult to establish misconduct under the *Corruption and Crime Commission Act 2003*, or a breach of discipline under the *Public Sector Management Act 1994*.
- Employees and contractors with access to confidential personal information are not necessarily screened for previous criminal histories prior to commencing employment.
- Criminal record screening is not regularly updated for all staff who have access to confidential personal information.
- The standard approach to criminal records screening may not capture all relevant offences. In addition to obtaining a National Police Clearance for applicable positions, each agency should consider whether further investigation is required of prospective employees to ensure their suitability for the work related requirements of the position.
- Agencies do not appear to have supervision arrangements to ensure that staff only access information that is relevant to their work.
- All agencies cover staff responsibilities to protect confidential information as part of their staff induction training program. Not all new employees are receiving the benefit of such training, or, if they are, this is not being recorded in their personnel files.
- On-going access to information regarding staff responsibilities could be improved by providing ready access to relevant policies and instructions, eg, on agency intranets, and providing refresher and update training to existing staff.

Recommendations – Security vetting

In keeping with the Commonwealth Protective Security Manual it is recommended that all employees and contractors with access to confidential personal information be background screened prior to commencing employment, and updated on a regular basis.

In addition to obtaining a National Police Clearance for applicable positions, it is recommended that each agency consider whether further investigation is required of prospective employees to ensure their suitability for the work-related requirements of the position.

Recommendation – Risk assessment and risk management

It is recommended that all public sector agencies include the risk of unauthorised access and disclosure when undertaking their risk management activities in accordance with Treasurer's Instruction 825 and Premier's Circular 2005/02.

Recommendations – Computer access

It is recommended that all agencies re-evaluate their information management systems to ensure that safeguards are in place to mitigate against unauthorised access and disclosure, including ensuring that:

- Audit tracking of access to confidential personal information is available and that access is monitored to identify anomalous use.
- Agencies review their supervision arrangements to ensure that staff only access information that is relevant to their work.
- Agencies include in their policy and induction manuals acknowledgement that unauthorised access and disclosure of confidential information is misconduct pursuant to the *CCC Act* and that suspected cases will be reported to this Commission.
- Agencies adopt pro-active measures to reduce the opportunities for unauthorised access and disclosure rather than responding to individual incidences in isolation.

Perceptions of Misconduct Survey Report

Introduction

The third term of reference of the Inquiry was to inquire and report into the adequacy of public officers' awareness of responsibilities to safeguard information. The Inquiry has addressed this term of reference through a survey of staff perceptions of access and disclosure of confidential personal information under a variety of circumstances using the following scenarios.

Survey scenarios

SCENARIO ONE

A prisoner tells a prison officer that his cousin is incarcerated in another prison and he thinks he is due to be released, but does not know when. The officer looks up the cousin's personal details on the prison system database. The release date is shown and is marked 'confidential – not to be disclosed'. He gives the prisoner the release date.

SCENARIO TWO

A woman complains to the media that she was denied a public housing rental property because she is an Indigenous Australian. The media contacts the public housing authority's regional office and speaks to the regional manager. The public housing authority's Public Relations Policy states that all media contact is to be managed through the Public Affairs Branch. The regional manager checks the woman's personal details in the authority's tenant database and tells the media that the actual reason for denying the tenancy request was because the woman had damaged several previous tenanted properties and had outstanding rental debts of over $5,000.

SCENARIO THREE

A public servant reads a news article about an ex-colleague who has won an award for bravery. The public servant is unable to locate the ex-colleague in the White Pages and does a search of his personal details on a government database. He then telephones him at home to congratulate him.

SCENARIO FOUR

A woman reverses into an unoccupied vehicle while shopping on the weekend. She leaves a message, including her contact details, on the windscreen and notes the vehicle make, model, and registration number. After one week, the owner has not contacted her, so she asks her neighbour, an employee at a vehicle registration authority, to find the owner's contact details. The neighbour accesses the owner's personal details on the vehicle registration database and provides the information to the woman, who subsequently contacts the person to arrange to pay for the damage.

SCENARIO FIVE

A group of ratepayers campaigning against the re-zoning of a small area of local bushland writes to local councillors, signing the document with the names of each member of the group. A councillor who supports the re-zoning wants to contact the ratepayers individually and looks up their contact details in the White Pages. The councillor is unable to find the details for one member and does not have access to council records about ratepayers. He asks an officer in the council's administration to provide the person's telephone number. The officer accesses the person's personal details on the ratepayer database and provides the councillor with the number. The councillor contacts the person, who subsequently complains to the council that the council administration released personal details without authorisation.

SCENARIO SIX

A police officer telephones a public servant requesting the address of a person who was a witness to a serious crime. The police officer identifies himself by name only and does not specify why he needs the information, however the public servant understands that there is a standing agreement for the agency to provide information from the agency's client database to assist police officers. The public servant accesses the person's personal details in the client database and provides the requested information verbally, and does not keep a record of the request.

SCENARIO SEVEN

A motor vehicle licensing officer knows that a colleague is having difficulty in getting her ex-husband to pay the correct amount of maintenance for their children. She knows that her colleague suspects that her ex-husband has undeclared assets in the form of valuable motor vehicles. To help her colleague, she accesses the ex-husband's details on the licensing database, displaying the details of vehicles registered in his name, and walks away from her computer, enabling the colleague to view the computer screen in her absence. The colleague uses the information in an application to the Child Support Agency to successfully obtain a change in the maintenance assessment.

SCENARIO EIGHT

A Department of Justice officer is approached by a neighbour who claims to be concerned about his 19-year-old daughter, who has been visiting a prisoner. The neighbour requests information about the prisoner's offence and release date. The officer is sympathetic to the neighbour's concerns and supplies the information from the prisons database, despite being aware that the neighbour and the prisoner are members of rival outlaw motorcycle gangs.

SCENARIO NINE

A government social worker has access to a sex offender register as part of her official duties. An acquaintance mentions that she has started dating a man who the social worker knows is registered for a previous conviction for a child sex offence. The acquaintance has a young child. The social worker knows that there are official processes for revealing personal details from the register but that these can take some time to implement. She tells the acquaintance about the man's previous conviction in order to protect the immediate safety of the child and does not report the disclosure to her employer.

SCENARIO TEN

A public officer working in population health has official access to a notifiable disease register. From time-to-time the officer accesses personal details in the register to find out if a new partner is listed as having a sexually transmissible disease. On one occasion, the officer finds out that a new partner does have an STD. As a consequence, the officer breaks off the relationship, but does not reveal why.

Survey approach

Five hundred and forty-five survey documents marked 'Perceptions of Misconduct: A Survey of People Working in the Public Sector' and accompanied by a letter from the Commissioner were couriered to each of the fieldwork agencies as follows on 30 December 2004:

- City of Melville (80 surveys)
- City of Rockingham (80 surveys)
- Department for Community Development (100 surveys)
- Department of Justice (60 surveys)
- Department for Planning and Infrastructure (145 surveys)
- Insurance Commission of Western Australia (80 surveys).

Completed surveys were returned by reply-paid post.

Survey sample

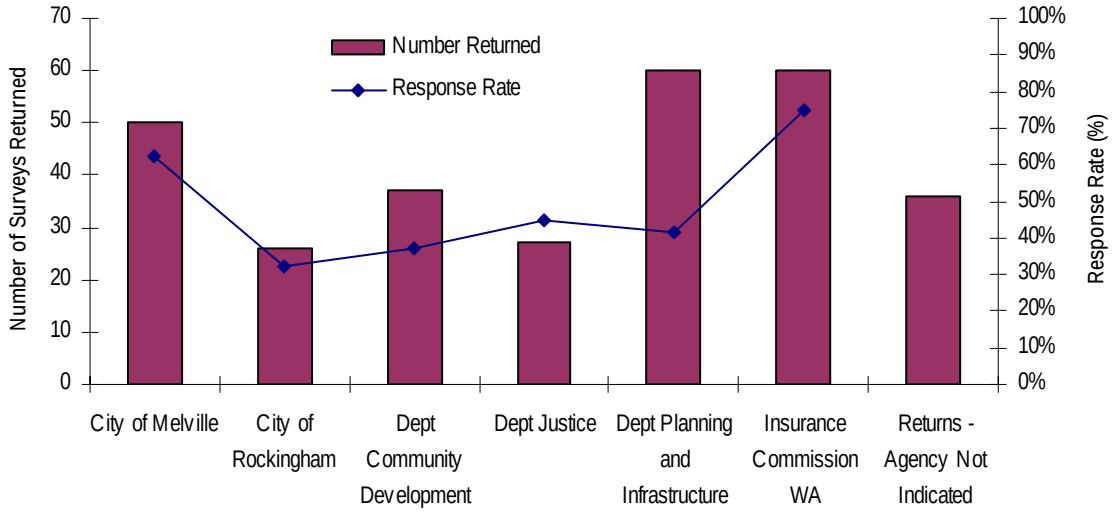
The survey sample was selected for delivery to a minimum of 60 respondents for each agency. Respondents for each agency were randomly selected from lists of staff with access to confidential personal information at the agencies or areas within the agencies that were the subject of the Inquiry fieldwork phase. The exceptions to this approach were:

- the Department of Justice, where surveys were forwarded to all staff of the two participating branch offices (Victoria Park and Maddington Community Justice Services); and

- the Insurance Commission, which was unable to produce a list of staff with access to confidential personal information without an unreasonable draw on resources. The Insurance Commission agreed to distribute the survey across the agency using a random selection from its internal staff list.

A total of 296 survey documents were returned, resulting in a response rate of 54%. Response rates for each agency are shown in Figure 2.

Figure 2: Response number and rate by agency.



Just over half (55%) of the respondents were female (See Figure 3). Respondent age approximated the age distribution in the WA public sector, although a slightly larger proportion of survey respondents were younger than 35 years (See Figure 4). Almost half (46%) of respondents had been employed in the public sector for less than ten years (See Figure 5).

Figure 3: Respondent gender.

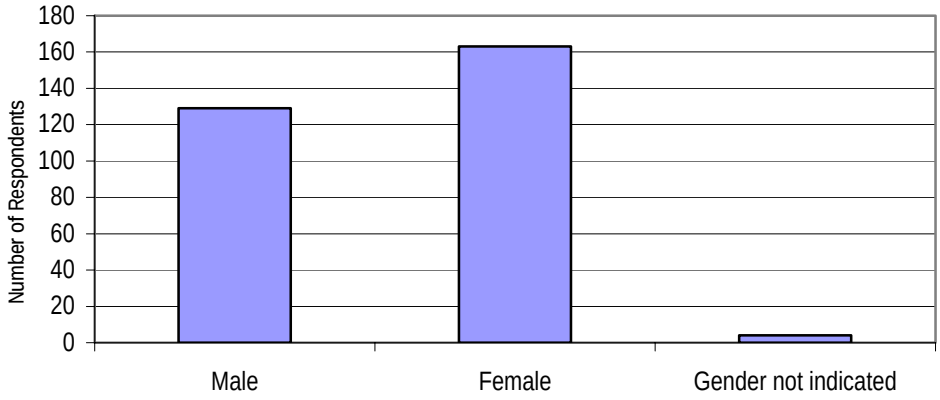


Figure 4: Respondent age.

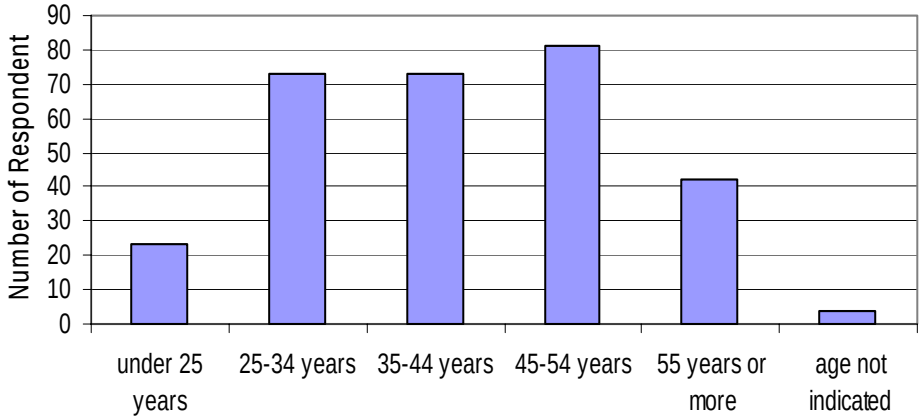
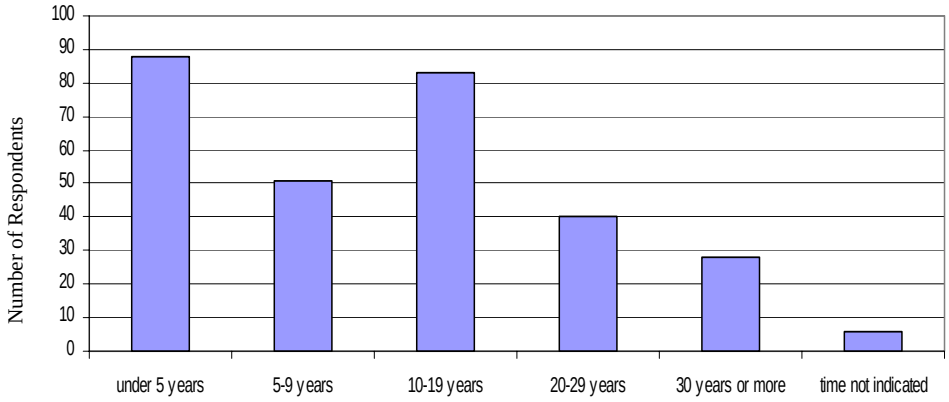


Figure 5: Time spent in the public sector.

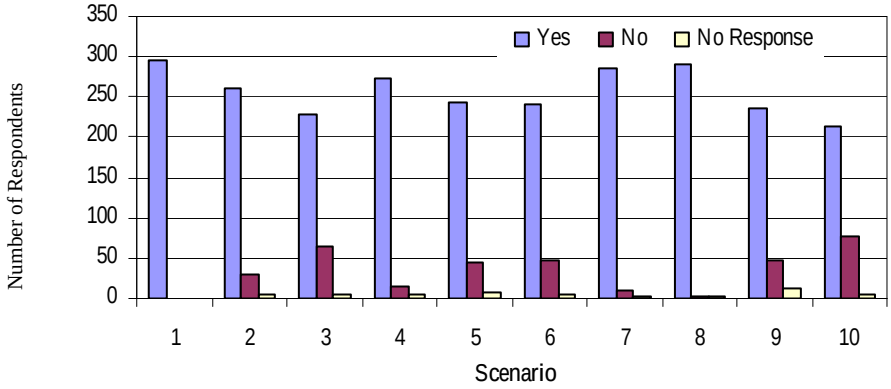


Results

Question One: Is the behaviour misconduct?

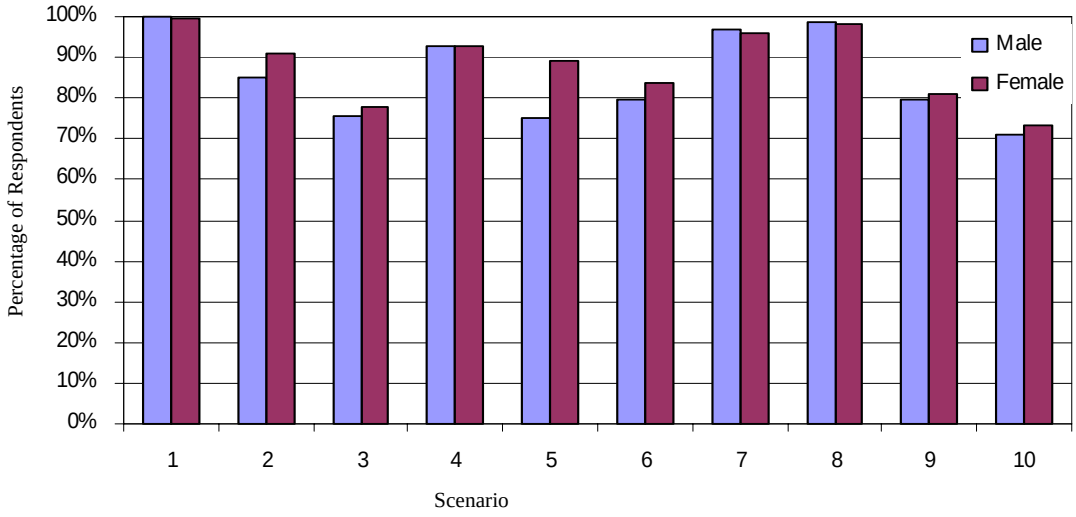
In each case, the majority of respondents indicated that they believed the behaviour to be misconduct. This varied from 72% of respondents for Scenario Ten and almost 100% of respondents for Scenario One.

Figure 6: Response to question one: 'Is the behaviour misconduct?' by scenario.



There was no significant difference in responses to Question One between men and women, with the exception of Scenario Five, where a larger percentage of women than men considered the behaviour to be misconduct (chi-square=12.280, df=1, p=0.0005).

Figure 7: Percentage of respondents answering 'Yes' to question one by gender.



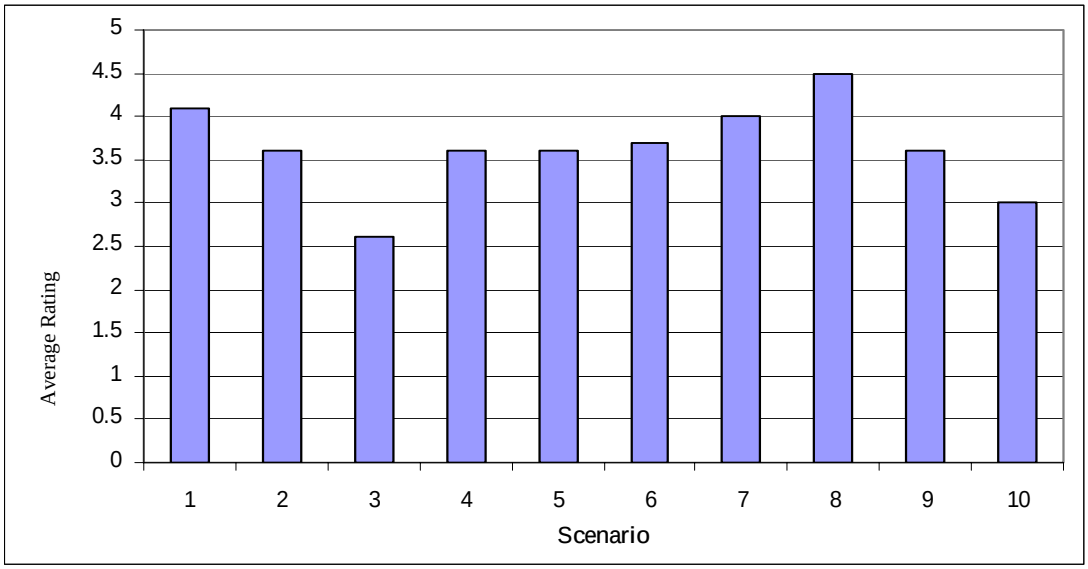
Question Two: How serious is the behaviour?

Respondents were asked how serious they rated the behaviour described in each scenario using the following scale:

◆ Not at all Serious ◆ Not very Serious ◆ Moderately Serious ◆ Very Serious ◆ Extremely Serious.

On average, respondents considered the behaviour described in Scenario Eight as the most serious (mean=4.5, df=287, p<0.0001) and Scenario Three as the least serious (mean=2.6, df=246, p<0.0001) (See Figure 8). Respondents did not differentiate between Scenarios Two, Four, Five, Six, and Nine in terms of perceived seriousness.

Figure 8: Average responses to question two by scenario.

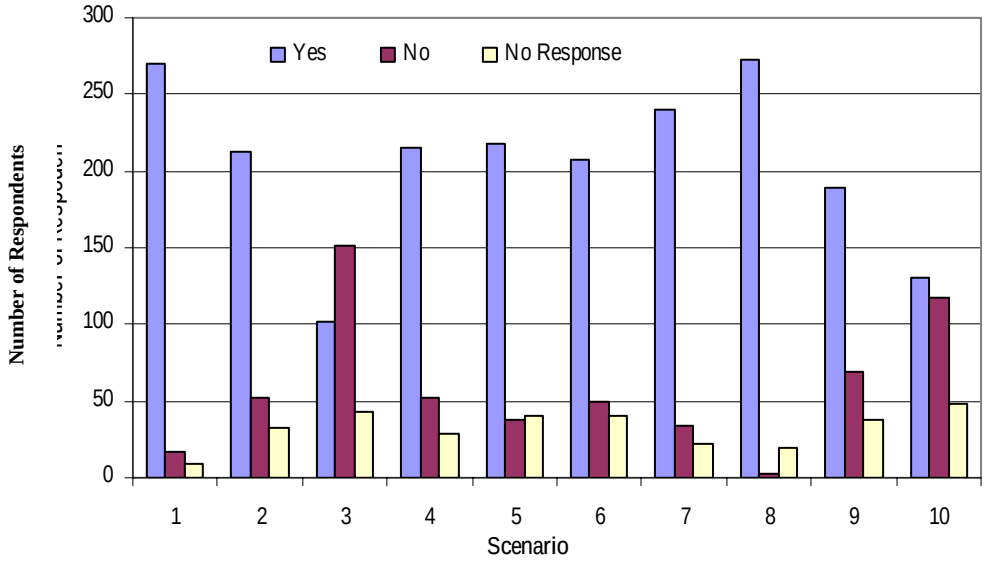


While there were some differences between ratings from respondents of different age, gender, and employing agency, these were statistical only ($p<0.05$) and the actual differences were not large.

Question Three: Would you report the behaviour?

Respondents indicated that they would be most likely to report the behaviour described in Scenarios One and Eight and least likely to report the behaviour described in Scenarios Three and Ten. This result is consistent with respondents' assessment of whether the behaviour was misconduct and the perceived seriousness of the behaviour.

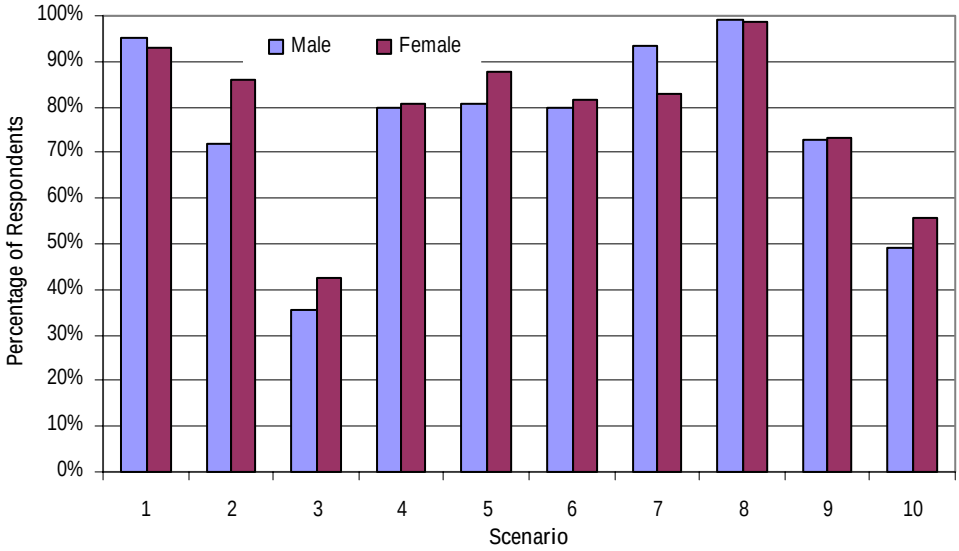
Figure 9: Responses to question three.



There was no significant difference in responses to Question Three between men and women, with the following exceptions:

- Scenario Two: a larger percentage of women than men would report the behaviour (chi-square=7.905, df=1, p>0.05);
- Scenario Seven: a larger percentage of men than women would report the behaviour (chi-square=6.435, df=1, p>0.05). (See Figure 9)

Figure 1: Responses to question three by scenario and gender.

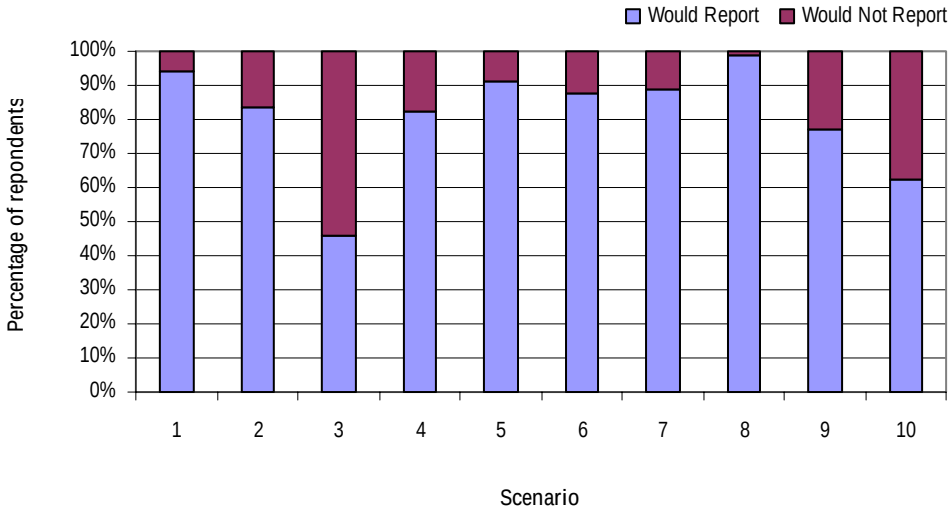


The majority of respondents who assessed the described behaviours as misconduct also indicated that they would report the behaviour (see Figure Ten). This was the case for all scenarios except Scenario Three, where 120 respondents indicated that they would not report the behaviour despite believing it to be misconduct. Respondents gave the following reasons for not reporting the behaviour:

- No personal gain was made by the public servant;
- No one was harmed.

These reasons were similar to reasons given for not reporting behaviours described in other scenarios. Some respondents to Scenario Three also indicated that, rather than reporting the person, they would prefer to counsel them on the appropriate use of information, suggest alternative methods of contacting people in future, and monitor their behaviour for future misuse of personal information.

Figure 2: Percentage of respondents answering 'yes' to question one who would and would not report the behaviour.



Opinions and issues

The survey results indicate that most respondents consider the behaviour described in the scenarios as misconduct, but that this percentage varies across the scenarios. Respondents were less likely to consider the behaviour to be misconduct where there was no perceived harm done (such as in Scenario Three) or the information was not disclosed to a third party (such as in Scenario Ten). Respondents tended to rate the scenarios as 'moderately' to 'very' serious. Again, assessment of the seriousness of the behaviour appeared to be related to the perceived harm or whether the information was disclosed to another person.

Except in the case of Scenario Three, respondents' intention to report the behaviour was related to whether they considered the behaviour to be misconduct. However, there was a proportion of respondents who indicated that they would not report the behaviour despite considering it to be misconduct. This proportion varied across the scenarios and appeared to be related to:

- the perceived harm resulting from the behaviour;
- whether the information was disclosed to a third party; and
- cases where the information was used to protect a third party or to 'right a wrong' or to serve some 'noble cause'.

Future training on managing and reporting misconduct in the workplace should incorporate the relevance of third-party disclosure on decisions to report misconduct. Training participants might also benefit from exploring reporting decisions in the context of complex scenarios, including:

- where there is no harm resulting from the misconduct; or
- where the misconduct presents an ethical dilemma, such as breaching confidentiality in order to protect the welfare of a third party.

Recommendation – On-line induction program

It is recommended that all new public sector employees be required to undertake an on-line computer-based induction program that provides information to them and instructs them in their responsibilities relevant to the handling of confidential information under such legislation as the *State Records Act*, *Freedom of Information Act*, *Public Sector Management Act*, *Occupational Health and Safety Act*, etc.

The Senior Executive On-line Induction program that is to be found on the Department of the Premier and Cabinet website is a useful model. Whereas that program is optional for new Senior Executive Service employees, what is recommended here is that program completion be compulsory and linked to probation periods and salary increments for new employees in the public sector. Successful completion of the program would generate a certificate that substantiates completion of the program.

Opinions and Recommendations

Opinions

At the commencement of this Inquiry a proposition was made that, in relation to the unauthorised access and disclosure of confidential personal information held on computer databases of public sector agencies, misconduct was occurring.

Nothing has been revealed during the course of this Inquiry that would dissuade this Commission from that view. It is this Commission's opinion that the relevant legislation and policy is inadequate and piecemeal, and improvements need to be made to the framework surrounding confidential personal information.

The selection processes currently in use across the public sector are inadequate in terms of providing a good appreciation of the backgrounds and character of applicants for vacant positions. Without this knowledge it is difficult to ensure that appropriate persons are being selected to meet the workrelated requirements of positions involving access to confidential information.

The training and supervision of public sector staff in the requirements to maintain confidentiality in the course of their employment are inadequate. The manner by which staff carry out their duties involving access to confidential personal information does not afford the necessary confidentiality that it ought. There is sufficient evidence to support the proposition that, in general, staff lack a firm appreciation of their responsibilities to safeguard information entrusted to their care. This includes a disinclination by some employees to report breaches of information security where they believe no personal benefit has been obtained, or where it serves some 'noble cause'.

Recommendations

The Criminal Code

The Commission recommends the amendment of the *Criminal Code* to consolidate offence provisions relating to unauthorised access and disclosure and to create a uniform set of provisions to address the inconsistencies of jurisdiction, definitions and penalties that currently exist. In seeking amendments to the Code the Commission further recommends that:

- Offences of unauthorised access and disclosure should prohibit dealing in the outcomes of unauthorised access at every point of the distribution chain, and include:

  - Unauthorised access;
  - Unauthorised use including 'browsing';
  - Unauthorised disclosure;
  - Procuring or bringing about unauthorised access or disclosure;
  - Attempting to procure or bring about unauthorised access or disclosure;
  - Soliciting or inducing another to make unauthorised access or disclosure;

- Offering to make unauthorised access or disclosure;
- Promoting oneself as capable of supplying information through unauthorised access or disclosure;
- Being in possession of confidential information without benefit of an excuse (with a reverse onus applying);
- Buying selling or otherwise dealing in confidential information; and
- Persons at second or third hand who gain access to unauthorised confidential personal information, knowing or ought to be knowing that it was made available through unauthorised access or disclosure.

- Unauthorised access and disclosure provisions be extended to embrace contractors and sub-contractors who are providing a service to a public sector agency and have access to confidential personal information as a consequence.
- In redrafting the *Criminal Code* the opportunity should be taken to clarify that a person who is an authorised user of a computer system can still be an unauthorised user if access is made beyond the scope of the authorised access.

Public Sector Management Act 1994

The Commission recommends the amendment of the *Public Sector Management Act 1994* to enable matters of unauthorised access and disclosure to be dealt with more appropriately. In seeking amendments to the *PSM Act* the Commission further recommends that:

- Sections of the Act dealing with substandard performance and discipline (Part 5) be redrafted to bring them into keeping with contemporary employment law and practices.
- Legislation be enacted to make public sector agencies not currently subject to the *Public Sector Management Act 1994* subject to that Act for disciplinary purposes. Section 239 of the *School Education Act 1999* provides a useful model:

> *Part 5 of the PSMA has effect as if in that Part references to:*
>
> *(a) an employee included –*
> *(iii) a member of the teaching staff; and*
> *(iv) an officer who comes within section 235(1)(c); and*
>
> *(b) an employing authority that is not the Minister (within the meaning in that Part) included references to the chief executive officer.*

- Clarification be made of the duty of public officers to maintain confidentiality of confidential personal information to better bring unauthorised disclosure within the provisions of s. 81 of the *Criminal Code*.

- An obligation be created for public sector agencies to provide an environment that mitigates the disclosure of confidential personal information through amending s. 29 of the *PSM Act* to specifically include a chief executive officer's responsibility for the protection of confidential personal information held by their agency.

Other legislation

In relation to other legislation, the Commission recommends that:

- Once the recommended amendments have been made to the *Criminal Code*, the existing provisions in agency or area specific legislation should be repealed in preference to the *Criminal Code*.
- The *Local Government Act* be amended to include a minimum code of conduct, the breaching of which would constitute a disciplinary offence.
- Regulation 9 of the Public Service Regulations be repealed once the *Public Sector Management Act* has been amended as recommended.
- Efforts currently in progress towards the adoption of a Privacy Act for Western Australia and the appointment of a Privacy Commissioner be continued.

Policy

It is recommended that existing policy in all its forms be reviewed by either the Department of the Premier and Cabinet, or the foreshadowed Privacy Commissioner, for the purposes of consolidation and to provide a sector-wide applicability. It is specifically recommended that:

- Policy be developed that covers all information held by government agencies, and which stipulates what information should be freely available to the public, is to be protected and not disclosed except where it is in the public interest to do so.
- Agencies review the level of authority that is required before releasing confidential personal information, with particular consideration to the amount of judgment and discretion allowed under agency disclosure policies.
- Treasurer's Instruction 825 be amended to include information held by an agency as a valuable asset that needs to be protected.
- The Department of the Premier and Cabinet review existing policy directives, such as Administrative Instructions 711 and 728, to update such where necessary by amending or repealing, and to ensure that public officers are aware of the content of these directives and of their responsibilities under them.
- A public sector oath be introduced for administering to all public sector employees, which establishes the duty and reinforces the requirement to maintain appropriate confidentiality of information. The wording of s. 183 of the *Corruption and Crime Commission Act 2003* might provide a suitable model.

Security vetting

It is recommended that all agencies in the public sector adopt the Commonwealth Protective Security Manual. It is particularly recommended that all employees and contractors with access to confidential personal information be background screened prior to commencing employment, and subsequently on a regular basis. Furthermore, in addition to obtaining a National Police Clearance for applicable positions, it is recommended that each agency consider whether further investigation is required of prospective employees to ensure their suitability for the work-related requirements of the position.[14]

Risk assessment and risk management

It is recommended that all public sector agencies include the risk of unauthorised access and disclosure when undertaking their risk management activities in accordance with Treasurer's Instruction 825 and Premier's Circular 2005/02.

Computer access

It is recommended that all agencies re-evaluate their information management systems to ensure that safeguards are in place to mitigate unauthorised access and disclosure, including ensuring that:

- Audit tracking of access to confidential personal information is available and that access is monitored to identify anomalous use.
- Agencies review their supervision arrangements to ensure that staff only access information that is relevant to their work.
- Agencies include in their policy and induction manuals acknowledgement that unauthorised access and disclosure of confidential information is misconduct pursuant to the *CCC Act* and that suspected cases will be reported to the CCC.
- Agencies adopt pro-active measures to reduce the opportunities for unauthorised access and disclosure rather than responding to individual incidences in isolation.

On-line induction program

It is recommended that all new public sector employees be required to undertake an on-line computer-based induction program that provides information to them and instructs them in their responsibilities relevant to handling of confidential information under such legislation as the *State Records Act*, *Freedom of Information Act*, *Public Sector Management Act*, *Occupational Health and Safety Act*, etc.

[14] This is to overcome the deficiency in the National Police Clearance in that it generally only checks for offences prosecuted under a criminal code.

Follow-up

The Corruption and Crime Commission intends conducting a follow-up review in approximately three years' time. This period is felt necessary to enable recommendations that have costs associated with their implementation time to flow through several budget cycles, and for those recommendations with long lead times, i.e. legislative change, to commence progress towards their adoption.

References

Chief Information Officer (CIO) Guideline, Office of Information and Communications Technology, NSW Department of Commerce (May 2002).

Commission of Government (1995) *Commission on Government Report No. 1: August 1995*, Perth.

Commonwealth Attorney General's Department (2000) *Commonwealth protective security manual*, Commonwealth Attorney General's Department: Canberra.

Confidential information: how to keep it confidential. A guide for councillors and CEOs, Crime and Misconduct Commission, 2004.

Criminal Justice Commission (2000) *Protecting confidential information: A report on the improper access to, and release of, confidential information from the police computer systems by members of the Queensland Police Service*. Criminal Justice Commission: Brisbane.

Ede, A. and Legosz, A. (2002) *Monitoring the ethical climate of organisations: A Queensland case study*, Crime and Misconduct Commission Research and Issues Paper No. 2.

Fielding, G. (1996) *Review of the Public Sector Management Act: A report to the Hon. RF Court MLA Minister for Public Sector Management*, Department of The Premier and Cabinet at www.dpc.wa.gov.au

Independent Commission Against Corruption (1992) *Report on unauthorised release of government information*, ICAC: Sydney.

Information Privacy Principles under the Privacy Act 1988 (Commonwealth), Office of the Federal Privacy Commissioner.

Information Security Guideline for NSW Government, Office of Information and Communications Technology, NSW Department of Commerce (2003).

Kelly, D. (Chairman) (1997) *Final report of the working party established to provide specific recommendations on amendments proposed by Commissioner Gavin Fielding*, Department of The Premier and Cabinet at www.dpc.wa.gov.au

Kennedy, G. (2004) *Report of the royal commission into whether there has been corrupt or criminal conduct by any Western Australian police officer*, State Law Publisher: Perth

Law Commission (1999) *Computer Misuse: Report 54*, Law Commission, Wellington.

McGinty, J. (2003) *Privacy legislation for Western Australia: Policy research paper,* Office of the Attorney General for Western Australia.

Meltham, D. (Chair) (1995) *In confidence: a report of the inquiry into the protection of confidential personal information held by the Commonwealth*, Standing Committee on Legal and Constitutional Affairs, House of Representatives, Australian Parliament.

Ombudsman of Western Australia, Western Australia Police Service and the Sellenger Centre (2001) *Reporting police misconduct*.

Organisation for Economic Co-operation and Development, 2002, *OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, at http://www.oecd.org/pdf/M00034000/M00034292.pdf

Practical Guide to Corruption Prevention.: Release of confidential information. Independent Commission Against Corruption.

Privacy Impact Assessment: A User's Guide. Office of the Corporate Chief Strategist. Ontario, 2001

Riley, J. (2004) *Privacy 'risk; in national ID plan*, *The Australian*, 21 January 2004.

Security in the Government Sector, Department of the Prime Minister and Cabinet, New Zealand, 2002.

Standards Australia & New Zealand Standards, 2001, AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management.*

Standards Australia & New Zealand Standards, 2004, AS/NZS 4360:2004 *Risk management.*

Standards Australia & New Zealand Standards, 2004, HB: 4360:2004 *Risk Management Guidelines – Companion to AS/NZS 4360:2004 Risk Management.*

Whitehead, N. (2004) *Review of the Public Sector Management Act 1994: A report to Hon J Kobelke MLA Minister Assisting the Minister for Public Sector Management*, Department of the Premier and Cabinet.

Appendix 1 Submissions Received

MEMBERS OF THE PUBLIC

Eight submissions received from private individuals.

COMMUNITY ORGANISATIONS

Mr R. Castiglione	Australian Services Union
Mr D. Smitherman	Injured Persons Action & Support Assoc. Inc.

ACADEMIC INSTITUTIONS

Dr T. Prenzler	Griffith University

GOVERNMENT AGENCIES

Mr P. Albert	Director General – Dept of Education & Training
Mr R. Cock QC	Director of Public Prosecutions
Superintendent F. Gere	Western Australia Police Service
Mr D. Pearson	Auditor General
Mr M. Wauchope	Director General – Dept of The Premier and Cabinet
Ms M. Murray	Commissioner for Public Sector Standards

Appendix 2 Information Privacy Principles (IPPs)

The following information privacy principles are derived from the *Privacy Act 1988* (Commonwealth). They provide a solid a minimum benchmark from which to work.

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

PRINCIPLE 1 - MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION

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.

PRINCIPLE 2 - SOLICITATION OF PERSONAL INFORMATION FROM INDIVIDUAL CONCERNED

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;

(c) 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:

   i. the purpose for which the information is being collected;

   ii. 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

iii. 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.

PRINCIPLE 3 - SOLICITATION OF PERSONAL INFORMATION GENERALLY

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:

(c) the information collected is relevant to that purpose and is up-to-date and complete; and

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

PRINCIPLE 4 - STORAGE AND SECURITY OF PERSONAL INFORMATION

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.

PRINCIPLE 5 – INFORMATION RELATING TO RECORDS KEPT BY RECORD-KEEPER

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:

i. the nature of that information;

ii. the main purposes for which that information is used; and

iii. 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 Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record 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 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:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

PRINCIPLE 6 - ACCESS TO RECORDS CONTAINING PERSONAL INFORMATION

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 Commonwealth that provides for access by persons to documents.

PRINCIPLE 7 - ALTERATION OF RECORDS CONTAINING PERSONAL INFORMATION

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 Commonwealth 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 provisions of a law of the Commonwealth; 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.

PRINCIPLE 8 - RECORD-KEEPER TO CHECK ACCURACY ETC OF PERSONAL INFORMATION BEFORE USE

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.

PRINCIPLE 9 - PERSONAL INFORMATION TO BE USED ONLY FOR RELEVANT PURPOSES

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.

PRINCIPLE 10 - LIMITS ON USE OF PERSONAL INFORMATION

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.

PRINCIPLE 11 - LIMITS ON DISCLOSURE OF PERSONAL INFORMATION

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 3 DPI – Arrangements to share information

The following schedule illustrates the wide variety of agencies, organisations and businesses that have access in some form or another to the information held on the databases of the Department of Planning and Infrastructure. The extent of this information sharing highlights the need to ensure that through legislation, policy and practice, there are mechanisms in place that protect the confidentiality of this information once it is in the hands of these external users.

Commonwealth	ATO
	Australia Post
	Centrelink
	Department of Family and Community Services/Child Support Agency
	Veterans Affairs
	ASIC
State	Fines Enforcement Registry
	Department of Justice
	Insurance Commission of WA
	Police
	DoCEP
	Main Roads
	DoIR
	Fisheries
	DTF
	Bailiffs
Local Government	79 WA Local Government Authorities
	Any public sector entity acting requesting assistance to enforce their parking/traffic by-laws
Other	Commonwealth Bank of Australia
	Zipform
	Leigh Mardon
	Automotive Data Services
	Licensys Pty Ltd
	Pingelly Brookton Community Financial Services Limited
	220 new and used car and motorcycle dealers
	Other state and territory licensing and registration authorities under the National Exchange of Vehicle and Driver Information System
	Administrators and Receivers in Bankruptcy

Appendix 4 FOI exempt agencies

- The Governor and the Governor's establishment.
- The Legislative Council or a member or committee of the Legislative Council.
- The Legislative Assembly or a member or committee of the Legislative Assembly.
- A joint committee or standing committee of the Legislative Council and the Legislative Assembly.
- A department of the staff of Parliament.
- The Auditor General and the Office of the Auditor General.
- The Corruption and Crime Commission.
- The Director of Public Prosecutions.
- The Information Commissioner.
- The Inspector of Custodial Services.
- The Parliamentary Commissioner for Administrative Investigations.
- The Parliamentary Inspector of the Corruption and Crime Commission.
- The Parole Board.
- The Supervised Release Review Board.
- The State Government Insurance Corporation.
- The Perth International Centre for Application of Solar Energy.
- Any Royal Commission or member of a Royal Commission.
- The Bureau of Criminal Intelligence, Protective Services Unit, Witness Security
- Unit and Internal Affairs Unit of the Police Force of Western Australia.
- The Internal Investigations Unit of Corrective Services.
- A person who holds an office established under a written law for the purposes of a body referred to in this Schedule.

Appendix 5 Table of statutes

- *Adoption Act 1994*
- *Children's Court Act 1988*
- *Community Services Act 1972*
- *Corruption and Crime Commission Act 2003*
- *Court Security Act 1999*
- *Criminal Code Compilation Act 1913*
- *Disability Services Act 1993*
- *Equal Opportunity Act 1984*
- *Financial Brokers Control Act 1975*
- *Freedom of Information Act 1992*
- *Health Act 1911*
- *Health Services (Conciliation and Review) Act 1995*
- *Human Reproductive Technology Act 1991*
- *Information Privacy Act 2000* (Victoria)
- *Insurance Commission of Western Australia Act 1986*
- *Interpretation Act 1984*
- *Local Government Act 1995*
- *Mental Health Act 1996*
- *Motor Vehicle (Third Party Insurance) Act 1943*
- *Occupational, Safety and Health Act 1984*
- *Prisons Act 1981*
- *Privacy Act 1988* (Commonwealth)
- *Public Sector Management Act 1994*
- *Public Service Regulations 1988*
- *State Records Act 2000*

Appendix 6 List of tables and figures

Tables

Figures

Appendix 7 Previous reviews

The following are summaries of a number of reviews conducted by other agencies into topics related to this inquiry. They are provided here to enable interested readers to develop greater awareness and understanding of the issues involved and of matters to consider in developing agency policy.

Management of confidential personal information in government electronic databases, **Office of the Auditor General in Western Australia, 2002.**

Contractual precautions that agencies should take in relation to contractor assess to confidential personal information include:

1. Individual, enforceable confidentiality agreements with contractors or between the agency and relevant employees or subcontractors of outsourced companies;
2. Agencies to have authority to routinely monitor compliance with the confidentiality requirements; and
3. Personal information held by an outsourced company to be destroyed once a service is completed and/or the contract is ended.
4. Monitoring of access for both read only and copy/download and change to data.
5. Managing Data Privacy in Centrelink. Australian National Audit Office, (Audit Report No.8 1999-2000) .

SUMMARY

The objective of this audit was to assess the systems put in place by Centrelink to protect data privacy. The audit reviewed the adequacy of the policies, procedures and the administrative framework associated with data privacy, and the computer systems that are used to store and disseminate data. The ANAO also examined compliance with legislative requirements.

*****

The Use of Confidentiality Provisions in Commonwealth Contracts. **Australian National Audit Office, (Audit Report No.38 2000-2001).**

SUMMARY

The audit's main objectives were to: examine the guidance on the use of confidentiality clauses in contracts and agencies' use of such clauses; develop criteria to assist agencies in determining what information in a contract is confidential; and assess the effectiveness of the existing accountability and disclosure arrangements for Commonwealth contracts.

*****

Personal Security – Management of Security Clearances. **Australian National Audit Office, (Audit Report No.22 2001-2002).**

SUMMARY

Personnel security, including the security clearance process, is a valuable and essential element of managing the risk inherent in allowing Commonwealth and other personnel access to sensitive information. This audit was designed to review security clearance and vetting policies and practices in a number of Commonwealth organisations and to consider if organisations were managing these processes effectively and efficiently and in accordance with Commonwealth policy, as outlined in the Protective Security Manual.

*****

Protection of Confidential Client Data from Unauthorised Disclosure – Department of Social Security. **Australian National Audit Office, (Audit Report No.23 1993-1994).**

SUMMARY

DSS has a strong commitment to the protection of client information from unauthorised release that includes operational staff awareness of their responsibilities and the implementation of a range of measures to strengthen data confidentiality. However, the nature of DSS's business creates a continuing risk of unauthorised disclosure of client information, particularly by its own officers. DSS should adopt a more structured approach to assessing the demand for its information.

DSS staff have widespread access to view and print client data on on-line computer systems. In the ANAO view there are options to reduce this vulnerability. Risk management requires a high priority be given to examine the extent to which user access, in particular to client address, may be narrowed and monitored through far wider use of audit trails of client record access. DSS also needs to have a more comprehensive and cohesive strategy for data confidentiality and to strengthen a number of data confidentiality measures. For example, temporary employees could have access to confidential information, sometimes without pre-employment checks.

*****

Protection of Confidential Client Data from Unauthorised Disclosure – Department of Social Security (Centrelink). **Australian National Audit Office, (Audit Report No.37 1997-1998).**

SUMMARY

The purpose of this follow-up audit was to report on action taken by the Department of Social Security and Centrelink in addressing the recommendations of Audit Report *No.23 1993-94 Protection of Confidential Client Information from Unauthorised Disclosure*.

The objectives were to: -

- ascertain the extent to which the recommendations of the original audit have been implemented;
- identify other changes made in relation to data confidentiality within the Social Security portfolio since 1993;
- assess the impact of the changes made; and identify any scope for further improvement.

*****

***Protection Security*. Australian National Audit Office, (Audit Report No.21 1997-1998).**

SUMMARY

The main objectives of the audit were to assess the management and administration of protective security across Commonwealth agencies and to identify, recommend and report better practice in security management. Particular attention was paid to: -

- compliance with Government policy, standards and guidelines; and
- the role of management in protective security; and the operation of security systems and practices.

The audit criteria and procedures to assess the management and administration of the individual organisations examined were largely based on the overall control framework of an organisation and the guidance provided in the current Commonwealth Protective Security Manual.

*****

***Operation of the Classification System for Protecting Sensitive Information*. Australian National Audit Office, (Audit Report No.7 1999-2000).**

SUMMARY
Previous audit reviewed, among other things, information security other than computer and communications security, against the policy and procedures outlined in the 1991 PSM. That audit found inconsistencies in the identification and marking of classified information and weaknesses in the handling and storage of classified information, as well as other breakdowns impacting on information security.

*****

***Physical Security Arrangements in Commonwealth Agencies*. Australian National Audit Office, (Audit Report No.23 2002-2003).**

SUMMARY
Physical Security Arrangements in Commonwealth Agencies, No.23 2002-2003 Protective Security involves the total concept of information, personnel, physical, information technology and telecommunications security. The Commonwealth's Protective Security policy is outlined in the Protective Security Manual (PSM). It provides specific guidance to agencies on the protection of the Commonwealth's assets, personnel and clients from potential security threats. This audit evaluated the protective security policies and practices of seven Commonwealth agencies to determine whether they had established an appropriate physical security control framework based on the principles outlined in Part E of the Commonwealth's Protective Security Manual. The ANAO also examined whether agencies had considered the risks of, and developed an appropriate policy statement on, the physical security arrangements for employees who work from home.

*****

***Management of Protective Security*. Australian National Audit Office, (Audit Report No.55 2003-2004).**

SUMMARY
The objective of the audit was to assess whether protective security functions in selected organisations were being effectively managed. In considering effectiveness, the audit assessed whether protective security arrangements: -

- were designed within the context of the business framework and the related security risks identified by the organisation; and
- provided an appropriate level of support for the organisation's operations and the delivery of its services.

*****

Integrity of the Electoral Roll. **Australian National Audit Office, (Audit Report No.42 2001-2002).**

SUMMARY

The Commonwealth electoral roll is managed by the Australian Electoral Commission ('AEC') and lists the names and addresses of people entitled to vote in federal elections. The objectives of the audit were twofold. The first objective was to provide an opinion on the integrity of the electoral roll, for the purpose of the audit, integrity was defined as accuracy, completeness, validity and security. The second objective was to examine the effectiveness of the AEC's management of the electoral roll in ensuring the roll's integrity.

*****

Integrity of the Electoral Roll. **Australian National Audit Office, (Audit Report No.39 2003-2004). Follow-up to 4.11 above.**

SUMMARY

The objective of this audit was to determine the progress made by the AEC in implementing the ANAO's recommendations, taking into account any changed circumstances, or new administrative issues, affecting implementation of those recommendations.

Appendix 8 Schedule 1 of the Public Sector Management Act 1994

Entities which are not organisations

- The Governor's establishment referred to in the *Governor's Establishment Act 1993*
- A department of the staff of Parliament referred to in the *Parliamentary and Electoral Staff (Employment) Act 1992*
- The electorate office of a member of parliament
- Any court or tribunal established under a written law and any judge or officer exercising a judicial function as a member of that court or tribunal
- The Police Force within the meaning of the *Police Act 1892*
- Curtin University of Technology established under the *Curtin University of Technology Act 1966*
- Edith Cowan University established under the *Edith Cowan University Act 1984*
- Murdoch University established under the *Murdoch University Act 1989*
- The University of Notre Dame established under the *University of Notre Dame Australia Act 1989*
- The University of Western Australia established under the *University of Western Australia Act 1911*
- Gold Corporation and Goldcorp Australia established under *the Gold Corporation Act 1987* and the Mint within the meaning of that Act
- The R&I Bank of Wester Australia Ltd within the meaning of the *R&I Holdings Act 1990*
- SGIO Insurance Limited established under the *SGIO Privatisations Act 1992*
- Any local government or the council of a local government or regional local government
- Racing and Wagering Western Australia established under the *Racing and Wagering Western Australia Act 2003*
- Any port authority established under the *Port Authorities Act 1999*
- Western Australian Land Authority established by the *Western Australian Land Authority Act 1992*
- Western Australian Treasury Corporation established by the *Western Australian Treasury Corporation Act 1995*
- Water Corporation established by the *Water Corporation Act 1995*
- Western Australian greyhound Racing Association established by the *Western Australian Greyhound Racing Association Act 1981*
- Western Power Corporation established by the *Electricity Corporation Act 1994*