The management of personal information - good practice and opportunities for improvement

Ombudsman Western Australia
Serving Parliament – Serving Western Australians

About this Report

This report is available in print and electronic viewing format to optimise accessibility and ease of navigation. It can also be made available in alternative formats to meet the needs of people with a disability. Requests should be directed to the Publications Manager.

Contact Details

Street Address
Level 12, 44 St Georges Terrace
PERTH WA 6000

Postal Address
PO Box Z5386
St Georges Terrace
PERTH WA 6831

Telephone: (08) 9220 7555 or 1800 117 000 (free call)
Facsimile: (08) 9325 1107
Email: mail@ombudsman.wa.gov.au
Web: www.ombudsman.wa.gov.au

ISSN: 1832-245X

First published by Ombudsman Western Australia on 28 March 2011

Contents

Ombudsman's Foreword

My office resolves complaints about the administrative decision-making of the public sector. Building on the knowledge gained from the investigation and resolution of these complaints, my office also undertakes a range of activities to improve public administration. These activities include publication of guidelines and other education activities, agency liaison as well as training and capacity building. One of the other key activities is undertaking investigations of certain aspects of public administration (often referred to as "own-motion" investigations). These own-motion investigations are intended to result in improvements to public administration in Western Australia that are evidence-based, proportionate, practical and consider the costs, as well as the benefits, of proposed improvements. In 2009 I established an Administrative Improvement Team with specific responsibility for undertaking these own-motion investigations.

This report is the result of an own-motion investigation of the management of personal information at three State Government agencies conducted by the Administrative Improvement Team.

I am very pleased that we observed many good practices at the three State Government agencies who participated in the investigation regarding the management of personal information. We also identified opportunities for improvement. In light of agreed good practice principles, combined with the good practices and opportunities for improvement observed during the investigation, we have developed a self-assessment checklist that can be used to assist all State Government agencies consider their management of personal information.

Chris Field
OMBUDSMAN

This page has been intentionally left blank.

1 Executive Summary

Personal information can be defined as information that identifies an individual or could identify that individual. State Government agencies properly require individuals to provide a range of personal information about themselves in order to deliver services, carry out law enforcement, administer regulations and perform other statutory functions. In short, effective and efficient service delivery, including protecting the well-being of individuals and the community, may require an agency to both collect, and disclose or share, personal information.

Inappropriate use of personal information is, however, as a matter of principle, wrong. Practically, it can compromise an individual's privacy leading to undesirable outcomes.

Alleged inaccuracy and inappropriate use of personal information is a source of complaint to the Ombudsman's office. These complaints provided an important base of evidence to suggest that this office should investigate the management of personal information by State Government agencies.

The objective of the investigation was to:

- determine whether the State Government agencies participating in the investigation (**the participating agencies**) are effectively managing personal information;
- if required, assist the participating agencies to improve their management of personal information; and
- identify good practice, lessons learnt and opportunities for improvement that might be useful to other State Government agencies in managing personal information.

To ensure a cost effective investigation with a timely outcome, the office determined to look at a sample of State Government agencies. To ensure that, as far as possible, the results of the investigation would have broader relevance to other State Government agencies, we used the following criteria to identify appropriate State Government agencies to participate in the investigation:

- the amount, range and sensitivity of personal information collected;
- the size of the program providing the service and the cross section of the community receiving the service; and
- the similarity of information collected and management processes to those of other State Government agencies.

State Government agencies considered for inclusion in the investigation did not need to meet all of the above criteria.

The office used a series of agreed good practice principles to assess the way in which the participating agencies were managing the personal information they collect and hold. These principles were based on national and state legislative requirements, agency specific legislation and internationally accepted good practice.

The office collected information about participating agencies' practices through:

- collection of details about the volume and type of personal information collected and held by each participating agency;
- a structured walk-through of agency processes for collecting, processing, storing, using, disclosing and destroying personal information; and
- fieldwork, including visits to branch offices, file and document reviews, interviews with key staff and contractors and reviews of internal controls.

At the completion of the fieldwork, the Ombudsman provided a preliminary report to the Chief Executive Officer of each participating agency setting out observations about the management of personal information at their agency and suggestions for administrative improvement. The participating agencies all received the observations positively. They have already implemented a number of the suggestions for administrative improvement and have taken steps to implement the other suggestions.

Feedback from the participating agencies regarding the preliminary reports was then taken into account in the development of this final report (**the Report**). The Report draws upon the observations and suggestions made in the individual agency reports, for the benefit of other State Government agencies. It sets these out as good practices identified during the investigation, together with observations about opportunities for improvement for the participating agencies. It is expected other State Government agencies will find it useful to reflect on both of these sets of findings.

To further assist State Government agencies, Chapter 5 of the Report consolidates the good practice principles, with examples of good practice and opportunities for improvement for the participating agencies, into a checklist for managing personal information. This checklist is designed to assist State Government agencies:

- to consider their own management of personal information against commonly accepted principles; and
- if required, to identify aspects of their own management of personal information that do not meet the principles and therefore represent opportunities for improvement.

1.1 Key findings

Each of the good practices and opportunities for improvement in the Report has been drawn from one or more of the participating agencies. While they were drawn from the participating agencies, not necessarily all were observed in each participating agency. A 'good practice' was considered to have been demonstrated when agency staff had effectively put one of the good practice principles into action. The opportunities for improvement identified relate specifically to the participating agencies and varied in terms of their significance.

1.1.1 Good practices observed

Examples of good practices observed included:

- there was an understanding of the importance of managing personal information effectively;
- maintaining the privacy of personal information was seen as part of day to day business;
- a clear, comprehensive and easily accessible privacy statement was available to individuals providing personal information;
- practical steps were taken to ensure that people from non-English speaking backgrounds understood the purpose and implications of providing their personal information;
- quality controls were used to improve the accuracy of personal information entered into agency Information and Communications Technology systems (**ICT systems**);
- there was an ongoing proactive approach to updating personal information to ensure it remained accurate;
- specific authorisation processes for the disclosure of personal information were established and used; and
- there were controls that were actively managed to protect personal information stored in both paper-based and electronic form from unauthorised access by both staff and people outside the agency.

1.1.2 Opportunities for improvement

The opportunities for improvement included that:

- individuals were at times not made aware of why their personal information was being collected;
- personal information that was not directly related or necessary to the agency's functions and activities or otherwise required by law was at times collected;
- some ICT systems did not facilitate the effective disposal of personal information when it was no longer necessary for service provision (and it would have otherwise been lawful to dispose of the information);
- there were instances where personal information recorded in paper form was not kept secure;
- safeguards over personal information held in electronic form included in the design of an agency ICT system, were at times not used in practice;
- measures to prevent inappropriate use and disclosure of personal information by third party service providers were at times not in place; and
- at times there was uncertainty about how to apply the good practice principles to the personal information of children.

Chapters 3 and 4 provide further detail about the good practices and opportunities for improvement observed during the investigation.

Chapter 5 utilises the examples of good practice and opportunities for improvement to create a checklist to assist State Government agencies to manage personal information.

2 Introduction

2.1 Objective of the investigation

The objective of the investigation was to:

- determine whether the participating agencies are effectively managing personal information;
- if required, assist the participating agencies to improve their performance in managing personal information; and
- identify good practices, lessons learnt and opportunities for improvement that might be useful to other State Government agencies in managing personal information.

To conduct the investigation, the office examined the management of personal information in three large programs conducted by three State Government agencies.

2.2 Definition of personal information

Personal information can be defined as information that identifies an individual or could identify that individual. This may include an individual's name, address(es), telephone numbers, email address(es), date of birth, employment details, bank account details, photographs and videos. It may also include such material as medical information, preferences, opinions and criminal history. Information does not have to include an individual's name to be personal information. For example, in some cases, an individual's date of birth and post code may be enough to identify them.[1]

The definition of personal information set out by the Australian Government Office of the Privacy Commissioner (**the Office of the Privacy Commissioner**), is:

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

The Office of the Privacy Commissioner also draws attention to certain types of personal information that are especially important to privacy, such as health or medical information. The *Privacy Act 1988* (Cth) (**the Privacy Act**) classifies this information as 'sensitive information', and specifically provides that sensitive information be managed with particular care.[2] While Western Australian government agencies are not subject to the *Privacy Act*, it provides a useful reference for agency practice.

[1] Office of the Privacy Commissioner - http://www.privacy.gov.au/aboutprivacy/what. Accessed 3 March 2011.

[2] Office of the Privacy Commissioner - http://www.privacy.gov.au/aboutprivacy/snapshot. Accessed 3 March 2011

2.3 Rationale for the investigation

2.3.1 Government needs to collect and use personal information to deliver services to the community

State Government agencies properly require individuals to provide a range of personal information about themselves in order to deliver services, carry out law enforcement, administer regulations and perform other statutory functions. For example, access to public utilities such as power and water requires a customer to provide their name and an address. In short, effective and efficient service delivery, including the protection of the well-being of individuals and groups of people, may require an agency to collect, and disclose or share, personal information.

The *Information Privacy Principles*,[3] which apply to Commonwealth Government agencies, recognise that government agencies may need to disclose personal information that they collect to third parties within and outside the public sector. In summary, the principles specifically provide for the disclosure of personal information in certain defined situations, namely:

- the individual concerned is reasonably likely to have been aware, or made aware, that information of that kind is usually passed to that person, body or agency;
- the individual concerned has consented to the disclosure;
- 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;
- the disclosure is required by or authorised under law; or
- 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.

To guide State Government agencies in this area, the Public Sector Commissioner has published a circular entitled *Policy Framework and Standards for Information Sharing between Government Agencies* (2009-29) (**the Circular**). The Circular recognises that:

> the community is demanding seamless services from agencies and expects positive outcomes from government spending. Structured sharing of important, and often sensitive, information is frequently needed to achieve improved community outcomes, benefits to clients and better coordinate services.[4]

[3] Office of the Privacy Commissioner - http://www.privacy.gov.au/law/act/ipp. Accessed 3 March 2011. Both the *National Privacy Principles* and *Information Privacy Principles* are currently being reviewed as part of proposed amendments to the Commonwealth *Privacy Act*.

[4] Public Sector Commissioner (WA) Circular *Policy Framework and Standards for Information Sharing between Government Agencies (2009-29)* at page 1. Available at http://www.publicsector.wa.gov.au/AgencyResponsibilities/PSCCirculars. Accessed 3 March 2011.

Participating agencies held large volumes of personal information. For example, to administer the programs examined, participating agencies held:

- the names and addresses of 1.38 million people;
- photographs of 123 440 people;
- banking details of 311 000 people; and
- information about the next of kin of approximately 40 000 people.

2.3.2 Concerns about inaccurate and inappropriate use of personal information

Alleged inaccuracy and inappropriate use of personal information is a source of complaint to the Ombudsman's office. These complaints provided an important base of evidence to suggest that this office should investigate the management of personal information by State Government agencies.

Similarly, if personal information held by an agency is inaccurate or unreliable, this may lead to wrong or poor decision-making. In the long term, concerns about the public sector's ability to maintain the accuracy and safeguard the confidentiality of personal information can result in decreased confidence in the public sector generally.

Complaints to the Ombudsman's office indicate that individuals recognise the need to provide information about themselves in order to receive government services. For example, people do not generally complain to the Ombudsman about the type of personal details they are required to provide to access a particular service. Complaints to the Ombudsman generally concern the alleged inappropriate use of personal information. The following cases illustrate the type of complaints the Ombudsman receives about alleged inappropriate use of personal information.

Case Study 1 – Inappropriate disclosure of personal information

A complainant to the Ombudsman's office alleged that her personal information (name, address, email and the names and ages of her children) was available publicly after she had enrolled her children online in a government-run program.

She contacted the State Government agency and was advised that, due to an error in the program, the webpage defaulted to the personal information of the previous person who had completed the online enrolment process when the next person entered the site to make an enrolment. The agency said that they would fix the problem but would not remove the web site or the web page while doing so.

After contact from the Ombudsman's office, the State Government agency agreed to remove the web page until the problem was fixed. The State Government agency also agreed to work with the complainant to resolve any outstanding issues with respect to potential breaches of privacy.

Complaints to the Ombudsman's office have also concerned the use of personal information that is inaccurate or incomplete. This has led to wrong or poor decision-making.

Case Study 2 – Decision based on inaccurate and incomplete information

A complainant to the Ombudsman's office alleged that her application for a loan had been unfairly refused by a State Government agency.

Enquiries by the Ombudsman revealed that the agency's decision to refuse the loan was based on incorrect and incomplete information due to an administrative error that disadvantaged the complainant's application. As a result, the State Government agency took action to rectify its error and the complainant's application for the loan was accepted and approved.

2.4 Methodology

Step 1 - Development of good practice principles

To assess performance, the Ombudsman's office developed a series of good practice principles for managing personal information by reference to agreed benchmarks (following consultation with key stakeholders). These are consistent with the *National Privacy Principles* and the *Information Privacy Principles* set out in the *Privacy Act*, and are discussed in more detail at section 2.5 below.

Step 2 – Focussing on a sample of State Government agencies

To ensure a cost effective investigation with a timely outcome, the office determined to look at a sample of State Government agencies rather than all agencies across the public sector on the basis that:

- the type of information collected by the sample State Government agencies, and the range of service recipients, were sufficiently typical of other agencies across the public sector to provide referable good practice and opportunities for improvement; and
- investigations by accountability agencies, such as this one, can impose a significant workload on State Government agencies, time that must be either additionally funded or is an opportunity cost to other services they provide. Accordingly, investigating a sample of agencies limits these costs.

The office used the following criteria to identify appropriate State Government agencies to participate in the investigation:

- the amount, range and sensitivity of personal information collected;
- the size of the program providing the service and the cross section of the community receiving the service; and
- the similarity of information collected and management processes to those of other State Government agencies.

Step 3 - Data collection

To better understand the personal information management processes used by the participating agencies and provide sound evidence on which to assess their performance, the office undertook the following data collection:

- collection of details about the volume and type of personal information collected and held by each participating agency;
- structured walk-through of agency processes for collecting, processing, storing, using, disclosing and destroying personal information; and
- fieldwork, including visits to branch offices, file and document reviews, interviews with key staff and contractors and reviews of internal controls.

Step 4 - Analysis, feedback and procedural fairness

At the completion of the data collection at each participating agency, the office:

- analysed the information collected through the fieldwork against the good practice principles to develop preliminary observations and identify suggestions for improvement specific to each agency;
- discussed our preliminary observations and suggestions for improvement with operational staff and senior managers at each agency and invited comments; and
- provided a preliminary report to the Chief Executive Officer of each participating agency setting out the office's observations about the management of personal information at their agency and suggestions for administrative improvement and providing, in accordance with the office's legislation and the principles of procedural fairness, an opportunity to comment on our preliminary report. Feedback from the participating agencies regarding the preliminary reports was then taken into account in the development of the Report.

Step 5 - Public reporting

The final step was to publish the Report drawing upon the observations and suggestions made in the individual agency reports, for the benefit of other State Government agencies. The Report sets these out as good practices identified during the investigation, together with observations about opportunities for improvement for participating agencies. It is expected other State Government agencies will find it useful to reflect on both of these sets of findings.

To provide for a more systematic self-assessment by agencies regarding how effectively they are managing personal information, at Chapter 5 the Report consolidates the good practice principles, examples of good practice, and opportunities for improvement for participating agencies, into a checklist for managing personal information. This checklist is designed to assist other State Government agencies to identify opportunities for improvement in their own operations by:

- considering their own management of personal information against commonly accepted principles;

- paying particular attention to the areas of potential improvement for their public sector colleagues within the participating agencies; and
- identifying aspects of their own management of personal information that do not meet the principles and therefore represent opportunities for improvement.

2.5 Good practice principles for managing personal information

Instructions and guidance for the management of personal information by State Government agencies are provided in a range of sources, including:

- legislation;
- the Western Australian Public Sector Code of Ethics;
- the Public Sector Commissioner's circulars on information sharing (discussed in Section 2.3.2 above) and computer security, as well as related materials on information security management;[5] and
- agency-specific policies and guidelines.

In addition, in Western Australia, some State Government agencies have informally adopted the *National Privacy Principles* or the *Information Privacy Principles*[6] as the basis for their policies for managing personal information.

For the purposes of this investigation, the office consolidated the various requirements and guidance available into a more concise set of good practice principles, and then consulted with key stakeholders on these principles.[7] These principles incorporate the good practice considered necessary to ensure the effective management of personal information and minimise its inappropriate use. The principles cover the aspects of managing personal information set out below.

[5] Public Sector Commission (WA) Public Sector Commissioner's Circular 2010-26 *Computer Information and Internet Security* - http://www.publicsector.wa.gov.au/AgencyResponsibilities/PSCCirculars/Lists/Circular/Attachments/287/2010-05%20Computer%20Information%20and%20Internet%20Security.pdf. Accessed 3 March 2011. Public Sector Commission (WA) – http://www.publicsector.wa.gov.au/SiteCollectionDocuments/Model Policies – Model Information Security Management Policy.doc. Accessed 13 December 2010.

[6] Office of the Privacy Commissioner - http://www.privacy.gov.au/law/act/ipp. Accessed 3 March 2011.

[7] See Attachment 1 for a full description of the good practice principles.

TABLE 1 – SUMMARY OF GOOD PRACTICE PRINCIPLES	
1. Collection	Only personal information necessary for service delivery is collected.
2. Use	Personal information is used only for the primary purpose it was collected, except in certain defined circumstances.
3. Accuracy	Personal information collected, used and disclosed is accurate and current.
4. Disclosure	Personal information is not disclosed to any people or organisations other than the individual concerned, except in certain defined circumstances.
5. Storage and security	Personal information is protected from misuse, loss and inappropriate access and disclosure.
6. Responsibility for the actions of service providers	Agencies ensure personal information provided to third party service providers is protected from inappropriate use and disclosure.
7. Access and correction	Agencies allow individuals reasonable access to their personal information, except in certain defined circumstances, and take reasonable steps to make requested corrections or deletions.
8. Transparency	The type of personal information that is collected and held, and the principles for its management, is accessible to clients and other interested members of the public.

This page has been intentionally left blank.

3 Good practices demonstrated by participating agencies

3.1 Introduction

This chapter sets out good practices that were demonstrated by participating agencies during the investigation.

Each of the examples of good practice in this chapter has been drawn from one or more of the participating agencies. While the good practice examples were drawn from the participating agencies, not necessarily all good practices were observed in each participating agency. A 'good practice' was considered to have been demonstrated when agency staff had effectively put one of the good practice principles into action.

Key points

- There was an understanding of the importance of effectively managing personal information.
- Maintaining the privacy of personal information was seen as part of day to day business.
- A clear, comprehensive and easily accessible privacy statement was available to individuals providing personal information.
- Practical steps were taken to ensure that people from non-English speaking backgrounds understood the purpose and implications of providing their personal information.
- Quality controls were used to improve the accuracy of personal information entered into agency databases.
- There was an ongoing proactive approach to updating personal information to ensure it remained accurate.
- Specific authorisation processes for the disclosure of personal information were established and used.
- There were controls that were actively managed to protect personal information stored in both paper-based and electronic form from unauthorised access by both staff and people outside the agency.

3.2 There was an understanding of the importance of managing personal information effectively

A good practice observed was an understanding of the importance of effectively managing personal information, the significance of this commitment to customers, and the impact that poor management practices could have on the integrity of, and confidence in, an agency.

This understanding was most often demonstrated through compliance with requirements for managing personal information, such as those set out in the good practice principles. We also observed a number of instances where extra precautions to protect certain types of particularly sensitive personal information had been taken, such as the personal information of children, medical information or information about domestic violence incidents or threats.

3.3 Maintaining the privacy of personal information was seen as part of day to day business

A good practice observed was an active commitment to the management of personal information as an integral part of an agency's day to day business, rather than as a separate responsibility. This included high-level guidance about when information could be disclosed and messages of reinforcement by the Chief Executive Officer in a Code of Conduct, the signing of confidentiality agreements upon joining the agency, the inclusion of policies and procedures for managing personal information in a thorough induction program, an employee 'Operations Manual' guiding day to day activities and regular refresher training on the topic.

Other examples of good practice at participating agencies included guidance for staff addressing aspects of managing personal information provided through the intranet and specific staff training prior to the launch of a new service, including information on privacy considerations for all staff involved in the delivery of the service.

3.4 A clear, comprehensive and easily accessible privacy statement was available to individuals providing personal information

A good practice observed was a clear privacy statement located on an agency's website, with links to its more comprehensive privacy policy and to the Office of the Privacy Commissioner's best practice guidelines.

3.5 Practical steps were taken to ensure that people from non-English speaking backgrounds understood the purpose and implications of providing their personal information

A good practice observed was a proactive approach to ensuring that clients from non-English speaking backgrounds understood what information they were required to provide in order to receive services, and the purpose and implications of providing this information. These arrangements included in-house interpreters in the most appropriate community languages at scheduled times each week, signs in community languages and 'wallet' cards that clients could show stating that they required an interpreter.

Another good practice observed was translating key information about the purpose and implications of providing personal information into the most appropriate community languages for their client base, and introducing the verbal delivery of the key information on the web-site.

3.6 Quality controls were used to improve the accuracy of personal information being entered into agency databases

Good practices observed included a variety of quality controls to check the accuracy and logic of personal information as it was being entered into a database. These controls included:

- automatic detection of anomalous or illogical dates;
- the use of mandatory fields to encourage consistency;
- automatic detection of invalid postcodes; and
- verification of names and addresses using logic programs.

3.7 There was an ongoing proactive approach to updating personal information to ensure it remained accurate

A good practice observed was a proactive approach to encouraging individuals to update their personal information by despatching forms on an annual basis to check that currently held personal details were up to date. Forms also clearly stated that people should notify any changes to personal details.

3.8 Specific authorisation processes for the disclosure of personal information were established and used

The good practice principles discussed at section 2.5 above provide the following guidance to Government agencies on the appropriate disclosure of personal information to third parties. In essence, Government agencies should only disclose personal information to third parties when:

- the individual concerned is likely to be aware that the information is usually passed to that person or organisation;
- the individual has consented to the disclosure;
- the agency has reasonable grounds to believe that the disclosure is necessary to lessen or prevent a serious or imminent threat to the life or health of an individual;
- the disclosure is required by or authorised under law; and
- the disclosure is necessary for criminal law enforcement, or enforcement of a law imposing a pecuniary penalty or for the protection of public revenue. The agency must record instances where personal information is used for these purposes.

Good practices we observed included:

- individuals had been asked to sign consent forms authorising the disclosure of their personal information to service providers, such as contractors and their sub-contractors. This measure assisted in ensuring that individuals were aware of the agencies' intention to disclose their personal information and had consented to its disclosure; and
- the establishment of a release process involving approval by a senior officer of all requests for release of personal information stored in information and communications technology systems.

3.9 There were controls that were actively managed to protect personal information in both paper-based and electronic form from unauthorised access by both staff and people outside the agency

Good practices observed included a range of controls to protect personal information from unauthorised access including:

- a requirement for staff handling certain types of personal information to sign a confidentiality agreement or provide a criminal records check;
- regular review of the currency of criminal records checks where this requirement was a condition of employment;
- separate secure storage for hard copy files containing sensitive personal information and access to these files restricted to only those staff who need access to undertake their work;
- password protection;
- a hierarchy of access permissions established and actively managed by supervisors to ensure that staff who have access to material of varying levels of sensitivity continue to need this access;
- a user tracking system of access to information held on ICT systems, with checks that this access was for appropriate reasons; and
- other controls such as deactivation after 30 days of user accounts that had not been accessed and verification of inactive accounts by agency human resources sections to check that users continue to be employed by the agency.

4 Opportunities for improvement

4.1 Introduction

This chapter sets out the opportunities for improvement in the management of personal information that have been identified for the participating agencies.

Each of the opportunities for improvement in the Report has been drawn from one or more of the participating agencies, although not necessarily all of the opportunities for improvement were observed in each participating agency. The opportunities for improvement also varied in terms of their significance.

Key points

- Individuals were at times not made aware of why their personal information was being collected.
- Personal information that was not directly related or necessary to the agency's functions and activities or otherwise required by law was at times collected.
- Some ICT systems did not facilitate the effective disposal of personal information when it was no longer necessary for service provision (and it would have otherwise been lawful to dispose of the information).
- There were instances where personal information recorded in paper form was not kept sufficiently secure.
- Safeguards over access by both staff and other people to personal information held in electronic form, included in the design of an agency's ICT system, were at times not used in practice.
- Measures to prevent inappropriate use and disclosure of personal information by third party service providers were at times not in place.
- At times there was uncertainty about how to apply the good practice principles to the personal information of children.

4.2 Individuals were at times not made aware of why their personal information was being collected

While good practices were observed in relation to this aspect of personal information management,[8] we also identified opportunities for improvement that included:

- insufficient information in application forms about the purpose of providing personal information and its possible uses (where the purpose and possible uses were not otherwise reasonably apparent from the context of the provision of the information); and

- a lack of key information in languages appropriate to their clients' demographic groupings, to ensure that these clients understood the purpose and implications of providing personal information.

A further opportunity for improvement observed included not advising individuals that aspects of their personal information (such as next of kin) could be used for purposes other than those discussed during the application process.

4.3 Personal information that was not directly related or necessary to the agency's functions and activities or otherwise required by law was at times collected

An opportunity for improvement observed was the collection and retention of information that was unnecessary for the purpose of service delivery, such as Tax File Numbers (TFNs).

The collection of TFNs generally occurred as a side effect of providing, for example, a copy of an Australian Taxation Office Notice of Assessment as proof of identity and income. However, individuals were at times neither advised that their TFN was not required nor that they could blank out this information before submitting the document.

The Office of the Privacy Commissioner has issued the following guidance on the use of TFNs and the incidental provision of TFNs:[9]

> 7. Incidental provision of tax file numbers
>
> 7.1 Where an individual is required by law, or chooses, to provide information which contains a tax file number for a purpose not connected with the operation of a taxation assistance agency or superannuation law:
>
> (a) that individual shall not be prevented from removing the tax file number; and
>
> (b) if the tax file number is not removed, the recipient shall not record, use or disclose the tax file number.

[8] See Chapter 3, section 3.5

[9] Office of the Federal Privacy Commissioner: *Tax File Numbers* - http://www.privacy.gov.au/law/act/tfn. Accessed 3 March 2011

4.4 Some ICT systems did not facilitate the effective disposal of personal information when it was no longer necessary for service provision (and it would have otherwise been lawful to dispose of the information)[10]

Opportunities for improvement observed were:

- the absence of an effective facility in some ICT systems for the deletion of personal information when it was no longer necessary for service provision but would have otherwise been lawful to dispose of the information. Although the information was made inactive, it remained in the agency's ICT system; and
- the retention of bank account details in some ICT systems when individuals changed their payment options from direct debit to another means even though they were no longer necessary.

4.5 There were instances where personal information recorded in paper form was not kept secure

An unexpected problem had arisen at a participating agency in relation to a new product considered as part of the investigation. This product was expected to involve largely electronic application forms but had also, in practice, generated large amounts of personal information in paper application forms. While security over information held in the agency's ICT system had been addressed, the agency had not maintained similar levels of security over paper-based information.

Opportunities for improvement observed included instances of:

- large volumes of paper forms and paper files containing personal information being transported between office locations without adequate controls to ensure that all forms and files arrived at their destination;
- paper forms awaiting data input being accessible to the public through an unsecured door; and
- paper forms containing personal information not stored securely at data processing facilities after processing.

4.6 Safeguards over access by both staff and other people to personal information held in electronic form, included in the design of an agency's ICT system, were at times not used in practice

Opportunities for improvement observed were:

- instances of risks to the security of data stored in agency ICT systems, including:
  - easy to guess passwords;

[10] In considering whether information collected and held by government can be deleted, agencies must give consideration to the *State Records Act 2000* and any other laws regulating disposal of government held information.

  - unauthorised user accounts;
  - limited access hierarchies for sensitive personal information; and
  - failure to remove access accounts belonging to former staff of the agency or current staff who no longer require access to this material.[11]
- safeguards that had been included in the design of ICT systems were at times either unused or were being overridden by staff in the field. These included:
  - all staff using the same username and password to access the main database;
  - user tracking systems and audit logs not being regularly reviewed;
  - an instance where recommendations made by a previous review of the agency's data security systems were not implemented; and
  - instances of irregular or no independent reviews of ICT systems.

4.7 Measures to prevent inappropriate use and disclosure of personal information by third party service providers were at times not in place

Opportunities for improvement observed in relation to the protection of personal information collected, held or accessed by third party service providers were instances of the following:

- inadequate specification of confidentiality requirements for the management of personal information by service providers, contractors, sub-contractors and agents;
- a lack of emphasis on compliance monitoring in contract specifications;
- irregular checks of the currency of police clearance certificates required for service provider employees; and
- service providers creating their own forms to collect personal information without the knowledge of the agency and without using practices such as privacy statements.

4.8 At times there was uncertainty about how to apply the good practice principles to the personal information of children

Discussions with agency staff also showed that, as a consequence of collecting personal information about children, there were occasions when parents or guardians requested access to this information. Such requests did not always fall under the ambit of good practice principle 4, which allows for disclosure when there is a serious threat to the health or life of an individual. In order to deal with these requests, agency staff felt compelled to resort to problematic practices, such as asking children (as young as six years of age) to give their permission for their parents to access their information or alternatively asking

[11] Similar risks had been identified by the Auditor General (WA) in his report *Information Systems Audit Report: March 2010* - http://www.audit.wa.gov.au/reports/pdfreports/report2010_02.pdf Accessed 3 March 2011

older children to give their permission for their parents to access their information while they were in the presence of the parent.

5 Checklist for effectively managing personal information

A final objective of the investigation was to consolidate the good practice principles, examples of good practice, and opportunities for improvement that might be useful to other State Government agencies in managing personal information into a 'checklist'. Some suggestions in the checklist are self-explanatory while others incorporate matters agencies might consider based on lessons learnt from our investigation. The checklist is designed to assist State Government agencies to:

- consider their own management of personal information against commonly accepted principles;
- note good practices observed in our investigation; and
- identify aspects of their own management of personal information that may present opportunities for improvement.

The checklist set out below is designed to be a guide. Not all the situations it envisages will apply equally to every State Government agency. An agency's needs, and any actions it might take as a consequence, will need to be considered in the context of:

- the amount, range and level of sensitivity of personal information collected;
- a risk assessment; and
- a cost/benefit analysis or similar assessment to determine the most appropriate action necessary to balance properly the protection of personal information and efficient and effective service delivery.

The checklist should also be considered in conjunction with the Public Sector Commission's guide to security of information held in electronic form '*A checklist for your agency's current information security practice.*'[12]

[12] Available at http://www.publicsector.wa.gov.au/SiteCollectionDocuments/Good%20Governance%20Guidelines%20-%20Checklist.pdf. Accessed 3 March 2011

CHECKLIST FOR EFFECTIVELY MANAGING PERSONAL INFORMATION

PRINCIPLE 1 – COLLECTION

Only personal information that is necessary for service delivery is collected

1.1 Does your agency from time to time check the type of personal information it collects to ensure that this information is necessary for the purpose of service delivery and directly related to your agency's functions or activities or otherwise required by law?

For instance, you might consider:

- Whether you inadvertently collect Tax File Numbers (**TFNs**) when you collect proof of identity or income documents even though TFNs are not necessary to deliver your services;
- Advising clients that they can delete their TFN from documents before providing them to you.

1.2 Does your agency from time to time review the way in which you collect personal information to ensure that your collection process is lawful and fair and that your staff are operating within these principles?

1.3 Does your agency clearly communicate to your clients what personal information you collect and why?

For instance, you might consider:

- A clear and comprehensive privacy statement that is easily accessible to, and understandable by, clients who are providing personal information;
- Ensuring your staff know how to explain to clients what this statement means when necessary;
- Taking steps to make this statement understandable to clients who do not understand English, are unable to read, or both by providing key information in community languages appropriate to the demographic grouping of your clients, and by using Translating and Interpreting Service National (TIS); and
- Consulting with key stakeholders to determine whether it would be more effective to find a verbal, rather than a written, means of providing this information to some clients.

PRINCIPLE 2 – USE

Personal information is used only for the primary purpose it was collected, except in certain defined circumstances

2.1 Does your agency from time to time check that you are using personal information only for the purpose it was collected?

2.2 Does your agency use personal information for secondary purposes, for example:

- Marketing;
- Strategic planning; or
- Statistical purposes?

2.3 If you answered yes to 2.2, has your agency taken steps to ensure that you are applying good practice for managing personal information in these circumstances?

PRINCIPLE 3 – ACCURACY

Personal information collected, used and disclosed is accurate and current

3.1 Does your agency check that personal information collected and used is accurate, up to date, complete and not misleading?

3.2 Does this checking process extend from collection points, through data entry to service delivery?

3.3 Is this process proportionate to the risks posed by the use of inaccurate information to your clients and to the efficiency and effectiveness of your agency?

For instance, you might consider efficient automatic checks to prevent errors when putting personal information into your agency's ICT system, such as dates of birth that cannot predate 1900 and postcodes that cannot be more than six characters.

3.4 Does your agency have a proactive process for updating information from time to time to ensure it is accurate prior to using it?

3.5 Does your agency have a safe, legal and effective process for deleting information that is no longer needed for service delivery or any other purpose, which also complies with your Recordkeeping Plan?

3.6 Does your agency use information from complaints about inaccurate information to continuously improve the accuracy of its personal information databases?

PRINCIPLE 4 – DISCLOSURE

Personal information is not disclosed to any people or organisations other than the individual concerned, except in certain defined circumstances

4.1 Has your agency clearly identified to staff when personal information can be disclosed and when it cannot?

For instance, you might consider an internal policy statement to guide staff on the circumstances in which they can:

- Disclose personal information, such as when disclosure would lessen or prevent a serious or imminent threat to the life or health of an individual; or
- Share personal information with other government agencies in line with the Public Sector Commissioner's Circular 2010-05.

4.2 Does your agency monitor whether your staff actually follow these requirements?

PRINCIPLE 5 – STORAGE AND SECURITY

Personal information is protected from misuse, loss and inappropriate access and disclosure

Security of personal information held in ICT Systems

5.1 Does your agency have controls to protect personal information from unauthorised access by staff and other people as an integral part of the design and operation of your ICT systems?

5.2 Does your agency check that the established controls are working in practice, including at any branches or other offices?

For instance, you might consider:

- Whether your ICT systems require unique passwords that are not easy to guess and are changed regularly;
- Monitoring whether your staff use this password protection in practice;

- A hierarchy of access permissions established and actively managed by supervisors to ensure that staff who have access to material of varying levels of sensitivity continue to need this access;
- A user tracking system of access to information held on IT systems, with checks that this access was for appropriate reasons;
- Other controls such as deactivation after 30 days of user accounts that had not been accessed and verification of inactive accounts by agency human resources sections to check that users continue to be employed.

Security of personal information held in paper form and on paper files

5.3 Is personal information stored on your agency's paper files subject to a similar level of security to that stored in your ICT systems?

5.4 Does your agency check whether the established controls over paper-based information are working in practice, including at any branch or regional offices?

5.5 Does your agency monitor the security of personal information on paper files when it is being transported between branch offices?

For instance, you might consider:

- Transporting paper files between branches only in secured bags;
- Using batch controls so that outgoing and incoming paper files are cross checked by a branch or section supervisor;
- Using a tracking system for paper files in transit between branches or other off site facilities.

Protection of sensitive personal information

5.6 Has your agency identified which personal information is sensitive personal information that might require additional safeguards?

For instance, you might consider assisting staff across your agency to classify the sensitivity of personal information appropriately and consistently.

5.7 Does your agency limit access to personal information to staff who 'need to know' for the purposes of service delivery?

For instance, you might consider:

- Tiered authorities to limit access to personal information held in your ICT systems to only those staff that 'need to know' for their work;
- Keeping paper files containing sensitive personal information in a separate secure location accessible by only authorised staff; and
- Requiring a senior officer or supervisor to approve access to sensitive personal information held on paper files.

PRINCIPLE 6 – RESPONSIBILITIES FOR THE ACTIONS OF SERVICE PROVIDERS

Agencies ensure personal information provided to third party service providers is protected from inappropriate use and disclosure

6.1 Does your agency actively ensure that third party service providers with access to personal information adhere to the good practice principles for its management?

For instance, you might consider:

- Including requirements for the management of personal information in contracts with service providers, their contractors, sub-contractors and agents;[13]
- Assessing whether the type of personal information held or accessed by service providers (such as information about children) necessitates particular requirements, such as criminal record checks for their staff;
- Including requirements that contractors principals should monitor compliance of their contractors, sub-contractors and agents.

PRINCIPLE 7 – ACCESS AND CORRECTION

Agencies allow individuals reasonable access to their personal information and take reasonable steps to make requested corrections or deletions

7.1 Does your agency inform individuals that they have the right to access their personal information and provide that access when requested?

7.2 Does your agency encourage clients to advise you when their personal information needs to be corrected or updated and have a simple process for this purpose?

For instance, you might consider:

- Including both written and verbal means for allowing clients to correct or update their personal information;
- Whether your ICT systems have a safe, legal (including compliance with the *State Records Act 2000*) and effective means of deleting personal information that is unnecessary or superseded.

7.3 Do your agency's processes include a cross-check of amendments to personal information held in ICT systems and in paper files to ensure consistency?

PRINCIPLE 8 – TRANSPARENCY

The type of personal information that is collected and held, and the principles for its management, are accessible to clients and other interested members of the public

8.1 Is a description of the type of personal information you collect and hold, and how you manage this personal information, easily accessible to your clients and other interested members of the public?

For instance, you might consider including a Personal Information Policy statement on your website.

8.2 Does your agency promote, from the highest organisational level, the importance of the effective management of personal information as an integral element of core business?

[13] See www.privacy.gov.au For draft contract provisions and other resources, See www.privacy.gov.au/governmentcontractors 3 March 2011

Attachment 1 - Good practice principles for managing personal information [14]

1. Collection of personal information	The agency collects only personal information that is: • to be used for a lawful purpose; • to be used for a purpose that is directly related to its functions or activities; and • necessary to perform these functions or activities. The agency collects personal information by lawful and fair means and not in an unreasonably intrusive way. The agency takes reasonable steps to ensure that the individual concerned is aware of: • the purpose for which the information is being collected; • the fact that the collection of the information is authorised by or required under law (if this is the case); and • any person to whom or organisation to which the agency usually discloses the information.
2. Use of personal information	The agency uses personal information only for purposes: • to which the information is relevant; and • which are directly related to the purpose for which the information was collected. The agency does not use personal information that was collected for a particular purpose for other purposes except in the following circumstances: • the individual consents to the use of the information for that other purpose; • the agency has reasonable grounds to believe that the use of the information is necessary to lessen or prevent a serious or imminent threat to the life or health of an individual; • the use of the information for that other purpose is required by or authorised under law; and • the use of the information is necessary for criminal law enforcement, or enforcement of a law imposing a pecuniary penalty or for the protection of public revenue. The agency makes a note of instances where personal information was used for these purposes.
3. Accuracy of personal information	The agency takes reasonable steps to ensure that the personal information it collects and uses is accurate, up to date, complete and not misleading. The agency does not use the information without taking reasonable steps to ensure that the information is accurate, up to date and complete.

[14] Based on Office of the Privacy Commissioner, *Information Sheet (Public Sector) 1 - Information Privacy Principles under the Privacy Act 1988* -http://www.privacy.gov.au/materials/types/infosheets/view/6541. Accessed 3 March 2011. Also based on other sources discussed in the body of the Report.

4. Disclosure of personal information	The agency does not disclose personal information to any person or organisation other than the individual concerned unless: • the individual concerned is likely to be aware that the information is usually passed to that person or organisation; • the individual has consented to the disclosure; • the agency has reasonable grounds to believe that the disclosure is necessary to lessen or prevent a serious or imminent threat to the life or health of an individual; • the disclosure is required by or authorised under law; and • the disclosure is necessary for criminal law enforcement, or enforcement of a law imposing a pecuniary penalty or for the protection of public revenue and the agency keeps a record of where personal information was used for these purposes. Where the agency discloses personal information in one of the above circumstances, the person or organisation to whom the information is disclosed should observe the good practice principles.
5. Storage and security of personal information	The agency puts reasonable security safeguards in place to protect the personal information it holds from loss, unauthorised access, modification, disclosure and other misuse.
6. Responsibilities for the actions of service providers	If it is necessary for the personal information to be given to a service provider, the agency does everything reasonably within its power to prevent unauthorised use and disclosure of the personal information by this provider.
7. Access to and correction of personal information	The agency: • allows individuals reasonable access to their personal information, unless this access would infringe the privacy of another party or would compromise criminal law enforcement, enforcement of a law imposing a pecuniary penalty or the protection of public revenue; and • takes reasonable steps to make corrections, deletions or additions to ensure that the information is accurate, up to date and complete and not misleading.
8. Transparency	The agency makes accessible to clients and other interested members of the public a description of the type of personal information it collects and holds and the principles for its management including: • the nature of the personal information it holds; • the purposes for which the personal information is used; • the classes of individuals about whom personal information is kept; • for how long it keeps personal information; • who is entitled to have access to the personal information and under what conditions; and • how to access personal information.

Ombudsman Western Australia
Level 12, 44 St Georges Terrace Perth WA 6000
PO Box Z5386 St Georges Terrace Perth WA 6831
Tel 08 9220 7555 • Freecall (outside metropolitan area) 1800 117 000 • Fax 08 9325 1107
Email mail@ombudsman.wa.gov.au • Website www.ombudsman.wa.gov.au