

Effective management of personal information is of vital importance to all agencies that are required to obtain personal information about individuals in order to deliver government services. Inappropriate use of personal information is, as a matter of principle, wrong. Practically, it can compromise an individual's privacy leading to undesirable outcomes for both the individual and the agency.

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.

Personal information is defined in the *Privacy Act 1988* as:

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

What are the 'good practice principles'?

The good practice principles detailed in these guidelines provide guidance to agencies on how to effectively manage personal information. They detail how and when personal information can be collected, how it should be used and disclosed, and storage and security of electronic, paper and sensitive information. The good practice principles also detail how individuals should be able to access that information and have it corrected if it is wrong and how agencies can ensure transparent management of personal information.

COLLECTION

Only collect personal information that is necessary for service delivery.

ACCURACY, ACCESS AND CORRECTION

Personal information collected, used and disclosed should be accurate and current. Individuals should be allowed reasonable access to their personal information and agencies should take reasonable steps to make requested corrections and deletions.

STORAGE AND SECURITY

Personal information should be protected from misuse, loss and inappropriate access and disclosure.

USE

Personal information should only be used for the primary purpose it was collected, except in certain defined circumstances. Agencies should ensure that personal information provided to third party service providers is protected from inappropriate use.

DISCLOSURE

Personal information should not be disclosed to any people or organisation other than the individual concerned, except in certain defined circumstances. Agencies should ensure that personal information provided to third party service providers is protected from inappropriate disclosure.

TRANSPARENCY

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

Good practices for the management of personal information

COLLECTION	
Overview	Agencies require individuals to provide a range of personal information about themselves in order to conduct their business functions. Agencies need to ensure that clients are aware that their personal information has been/needs to be collected, why it is has been/needs to be collected, where the information is stored and who has access to it.
Checklists: Type of information	Does your agency from time to time check the type of personal information it collects to ensure: <ul style="list-style-type: none"> <input type="checkbox"/> being collected for a lawful purpose? <input type="checkbox"/> being used for a purpose that is directly related to the agency’s functions or activities? <input type="checkbox"/> necessary to perform these functions or activities?
Process of collection	Does your agency from time to time review the way in which you collect personal information to ensure that your collection process is: <ul style="list-style-type: none"> <input type="checkbox"/> lawful and fair? <input type="checkbox"/> staff are operating within the good practice principles? <input type="checkbox"/> not collecting information in an unreasonably intrusive way
Communication	Does your agency clearly communicate to your clients: <ul style="list-style-type: none"> <input type="checkbox"/> that the personal information has been collected? <input type="checkbox"/> the purpose for which the information is being collected? <input type="checkbox"/> that the collection of the information is authorised by or required under law (if this is the case); and <input type="checkbox"/> that the agency may disclose the information to others to deliver its functions or activities to the individual?
Suggested actions	<ul style="list-style-type: none"> • Consider providing clients with a clear and comprehensive privacy statement that is easily accessible to, and understandable by, clients who are providing personal information; • Ensure your staff know how to explain to clients what the privacy statement means when necessary; and • Take steps to make the 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). Consider if you need to find a verbal, rather than a written, means of providing this information to some clients.

ACCURACY, ACCESS AND CORRECTION	
Overview	Agencies should have processes in place to check that personal information about their clients is accurate, complete and current.
Checklist for Accuracy	Does your agency: <ul style="list-style-type: none"> <input type="checkbox"/> check that personal information collected and used is accurate, up to date, complete and not misleading? <input type="checkbox"/> have a checking process in place to extend from collection points, through data entry to service delivery and 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? <input type="checkbox"/> have a proactive process for updating information from time to time to ensure it is accurate prior to using it? <input type="checkbox"/> inform individuals that they have a right to access their personal information and how they can provide updates as required?
Checklist for Access & Correction	Does your agency: <ul style="list-style-type: none"> <input type="checkbox"/> have a safe, legal and effective process for deleting information that is no longer needed, which also complies with your Recordkeeping Plan? <input type="checkbox"/> have processes in place to cross-check amendments to personal information held in Information and Communication Technology (ICT) systems and in paper files to ensure consistency? <input type="checkbox"/> use information from complaints about inaccurate information to continuously improve the accuracy of its personal information databases?

ACCURACY, ACCESS AND CORRECTION, CONTINUED

Suggested actions

- Consider implementing 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.
- Allow clients to correct/update their personal information verbally and/or in writing.
- Ensure your ICT systems have a safe, legal and effective means of deleting personal information that is unnecessary or superseded.

STORAGE AND SECURITY

Overview

Agencies should take steps to ensure that personal information is protected from misuse, loss and inappropriate access and disclosure. Additional consideration should be given to the protection of sensitive personal information. Storage and security practices should apply to personal information stored in both ICT systems and paper files.

Checklists: ICT Systems

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

Paper form and on paper files

- Is personal information stored on your agency's paper files subject to a similar level of security to that stored in your ICT systems? Does your agency check whether the established controls over paper-based information are working in practice, including at any branch or regional offices?
- Does your agency monitor the security of personal information on paper files when it is being transported between branch offices?

Protection of sensitive personal information

- Has your agency identified which personal information is sensitive personal information that might require additional safeguards and does your agency give staff guidance to classify this information appropriately and consistently?
- Does your agency limit access to personal information to staff who 'need to know' for the purposes of service delivery?

Suggested actions

- Ensure your ICT systems require unique passwords that are not easy to guess and are changed regularly and monitor whether staff use this password protection;
- Implement a hierarchy of access permissions which are actively managed by supervisors to ensure that only those staff that 'need to know' for their work have access;
- Have a user tracking system of access to information held on ICT systems, with checks that this access was for appropriate reasons;
- Implement other controls such as deactivation after 30 days of user accounts that have not been accessed and ensure verification of inactive accounts by agency human resources sections to check that users are still employed;
- Transport paper files between branches or to off-site facilities in secured bags and use a tracking system for paper files in transit;
- Use batch controls so that outgoing and incoming paper files are cross checked by a branch or section supervisor; and
- Keep paper files containing sensitive personal information in a separate secure location.

USE

Overview

Agencies should only use the personal information they collect about clients for the purpose for which it was collected. In some circumstances, it may be appropriate that the information is used for secondary purposes such as marketing, strategic planning or statistical purposes.

Checklists: Agency use

- Does your agency:
- check that you are using personal information only for the purpose it was collected or for authorised secondary purposes?
 - where personal information is used for secondary purposes (for example, marketing, strategic planning, or statistical purposes) take steps to ensure that good practice is applied for managing personal information in these circumstances?

USE, CONTINUED	
Third party use	<input type="checkbox"/> Does your agency actively ensure that third party service providers with access to personal information adhere to the good practice principles for its management and protect it from inappropriate use?
Suggested actions	<ul style="list-style-type: none"> Assess 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; Consider including requirements for the management of personal information in contracts with service providers, their contractors, sub-contractors and agents; and Determine if there is a need to include requirements that contractors' principals should monitor compliance of their contractors, sub-contractors and agents.

DISCLOSURE	
Overview	Agencies may need to disclose personal information that they collect to third parties within and outside the public sector in order to effectively deliver services.
Checklists: Agency	<input type="checkbox"/> Does your agency clearly identify to staff when personal information can be disclosed and when it cannot, and does it monitor whether staff follow these requirements?
Third party	<input type="checkbox"/> Does your agency monitor whether third party service providers clearly identify to staff when personal information can be disclosed and when it cannot, and does it monitor whether staff follow these requirements?
Suggested actions	<ul style="list-style-type: none"> Consider publishing an internal policy statement to guide staff on the circumstances in which they can: <ul style="list-style-type: none"> 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.

TRANSPARENCY	
Overview	The type of personal information that is collected and held, and the principles for its management, should be easily accessible to clients and other interested members of the public. Agencies should promote, from the highest organisational level, the importance of the effective management of personal information as an integral element of core business.
Checklists: Access	<input type="checkbox"/> Does your agency provide a description of the type of personal information you collect and hold, and how you manage this personal information and is this description easily accessible to your clients and other interested members of the public?
Promotion	<input type="checkbox"/> 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?
Suggested actions	<ul style="list-style-type: none"> Consider publishing a Personal Information Policy statement on your website.

Other resources

The following publications are available on our website at www.ombudsman.wa.gov.au to assist agencies in the management of personal information:

- Checklist for Managing Personal Information*
- Good practice principles for the management of personal information*
- The Ombudsman's Report ***The management of personal information – good practice and opportunities for improvement***

Further information

Other useful resources for the effective management of personal information can be found on Office of the Australian Information Commissioner's website at www.privacy.gov.au. Information about appropriate release of personal information in Western Australia can be found on the Office of the Information Commissioner website at www.foi.wa.gov.au.

Ombudsman Western Australia