Australian Privacy Principles

Privacy principles govern a data lifecycle

The Privacy Act 1988 includes 13 Australian Privacy Principles (APPs). They govern standards, rights and obligations for handling personal information by organisations and agencies covered by the Act, called APP entities.

> **Important:** The APPs are principles-based and technology neutral. Apply the relevant principle to the evidence rather than assuming that every organisation or every scenario is covered in exactly the same way.

This page supports Digital Solutions analysis, not legal advice. The Office of the Australian Information Commissioner provides the current official guidance.

What counts as personal information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Context matters: several ordinary data points may identify someone when combined.

- Name, address, account ID and identifiable photo may be personal information.
- Location history or device data may become personal information when linked to a person.
- **Sensitive information** includes particular higher-risk categories and generally receives stronger protection.

- **De-identified data** has identifying information removed or altered so individuals are no longer reasonably identifiable; removing only names may be insufficient.

Personal, sensitive or de-identified?

Analyse these examples.

1. A named student's allergy record.
2. A public count of 318 visits with no individual records.
3. A dataset without names that contains exact birth date, postcode and rare medical condition.

Check your answer

1. Personal and sensitive information.
2. Aggregated data that is likely de-identified if no individual can reasonably be identified.
3. Potentially identifiable personal and sensitive information because the combination may single out a person. Removing names alone does not guarantee de-identification.

The 13 APPs at a glance

Stage	APP	Focus
Consider privacy	1	Open and transparent management of personal information
	2	Anonymity and pseudonymity
Collect	3	Collection of solicited personal information
	4	Dealing with unsolicited personal information
	5	Notification of collection
Use and disclose	6	Use or disclosure of personal information
	7	Direct marketing

Stage	APP	Focus
8	Cross-border disclosure	
9	Government-related identifiers	
Maintain integrity	10	Quality of personal information
	11	Security of personal information
Individual rights	12	Access to personal information
	13	Correction of personal information

APPs 1 and 2: plan and be transparent

APP 1 concerns open and transparent management, including an up-to-date privacy policy and practices for handling inquiries or complaints. **APP 2** concerns giving individuals the option of anonymity or a pseudonym where practicable, subject to limited exceptions.

A public event timetable may not need a user's identity just to show session times. A personalised ticket purchase may require information to complete the transaction.

Is identity necessary?

A council feedback form requires full name, date of birth and a verified account before a person can suggest a new park bench location.

Determine the most relevant APP concern and **Explain** why.

View a sample solution

APP 2 is relevant because the task appears capable of accepting anonymous or pseudonymous feedback. Requiring verified identity and birth date may be unnecessary unless the council can establish a particular need or legal requirement.

APPs 3, 4 and 5: collect carefully

- **APP 3:** concerns when solicited personal information may be collected, with higher standards for sensitive information.
- **APP 4:** concerns personal information received without being requested and whether it could have been collected; information may need to be destroyed or de-identified where lawful and reasonable.
- **APP 5:** concerns taking reasonable steps to notify people about collection matters, such as who is collecting, purpose and likely disclosures.

> **Data minimisation:** collect only information reasonably needed for the purpose. “It might be useful later” is not a specific purpose.

Analyse collection

A workshop booking needs a name and contact method. The form also requires annual income, precise live location and a medical history without explaining why.

Analyse the collection using APPs 3 and 5.

View a sample solution

The name and contact method have a clear booking purpose. The other fields appear excessive for that purpose, and medical history is sensitive. The collection notice should explain the collector, purpose and handling, but notification alone does not make unnecessary collection appropriate.

APPs 6 to 9: control use and disclosure

- **APP 6:** limits use or disclosure for another purpose unless an exception applies, such as consent or a related expected purpose in relevant circumstances.
- **APP 7:** sets conditions around direct marketing and mechanisms to stop receiving it.
- **APP 8:** concerns reasonable steps before disclosing personal information overseas and possible accountability for handling by the recipient.

- **APP 9:** limits adopting, using or disclosing government-related identifiers as an organisation's own identifier.

Purpose is central. Information collected to deliver a service should not silently become unrestricted material for an unrelated purpose.

Primary and secondary purposes

A sports app collects an email to send booking confirmations. It later supplies emails and exercise histories to an unrelated advertiser.

Determine the primary and secondary purposes and the main APP concern.

Check your answer

The primary purpose is managing bookings and confirmations. Advertising is a secondary purpose, and disclosure to the unrelated advertiser raises an APP 6 concern. APP 7 may also be relevant to direct marketing. A complete legal conclusion would depend on facts such as notice, consent, expectations and applicable exceptions.

APPs 10 and 11: quality and security

APP 10 concerns reasonable steps to ensure personal information is accurate, up to date, complete and relevant for its use or disclosure. **APP 11** concerns reasonable steps to protect information from misuse, interference, loss and unauthorised access, modification or disclosure.

APP 11 also includes considering destruction or de-identification when personal information is no longer needed, subject to exceptions such as legal retention requirements.

Evidence	Main concern	Possible design response
Old emergency contact is used	APP 10 quality	Prompt review and show last-confirmed date

Evidence	Main concern	Possible design response
All staff can export every record	APP 11 security	Least-privilege access, authentication and audit logs
Obsolete copies retained indefinitely	APP 11 lifecycle	Documented retention and secure disposal process

APPs 12 and 13: access and correction

APP 12 concerns an individual's access to personal information held about them. **APP 13** concerns reasonable steps to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading for the purpose for which it is held.

Access does not mean every person can browse all records. It concerns an individual accessing information about themselves through an appropriate process, subject to applicable grounds and procedures.

Design for rights

A membership app displays a wrong date of birth but has no correction request or privacy contact.

Recommend a refinement and **Justify** it using APP 13.

View a sample solution

Provide an authenticated correction-request process and visible privacy contact. It should identify the field, accept supporting information where appropriate and communicate the outcome. This supports reasonable correction of inaccurate information and prevents the wrong birth date continuing to affect decisions.

Construct an APP analysis

Evidence: what information is handled and what happens to it. **Principle:** the most relevant APP and its focus. **Consequence:** why the handling matters to the person. **Refinement:** a specific change that addresses the issue.

Avoid absolute legal claims: stimulus may not establish whether an entity is covered or whether an exception applies. State what the evidence raises or suggests unless the necessary facts are supplied.

Independent practice: youth activity platform

A community organisation's platform:

- requires exact birth date and home address to view a public activity timetable
- shows a brief notice saying only “We collect data”
- uses booking emails to advertise an unrelated paid service
- lets every volunteer download participant contact and health details
- retains cancelled-account data without a documented reason or review date
- provides no way for a participant to view or correct their information.

Analyse four different issues. For each, identify the evidence, relevant APP, possible consequence and a specific refinement.

View a sample solution

- **APPs 2 and 3:** requiring identity details merely to view a public timetable appears unnecessary. Permit anonymous access and collect booking data only when needed.
- **APP 5:** the notice does not explain collection purpose and handling. Provide a clear collection notice at or before collection.
- **APPs 6 and 7:** unrelated advertising is a secondary use and direct marketing concern. Separate the purpose, consider applicable permission and provide a clear way to stop marketing.
- **APP 11:** every volunteer can export sensitive and contact data. Apply individual authentication and least-privilege roles, with access limited to necessary records.
- **APP 11:** indefinite retention increases exposure. Establish lawful retention rules and securely destroy or de-identify information no longer needed.

- **APPs 12 and 13:** provide processes for authenticated access and correction requests.

Revision #5
Created 2026-10-06 00:40:29 UTC by Mr Napper
Updated 2026-10-06 01:32:12 UTC by Mr Napper