

Using the University's Privacy Collection Notices

Last updated: August 2026 | Version 1.0

Purpose

This guidance helps University teams use the University's approved privacy collection notices, including the student, staff and alumni notices, as operational references. It does not replace the Privacy Policy, Privacy Management Plan, a project-specific privacy impact assessment or legal advice.

1. What the notices do

The notices explain, at a whole-of-lifecycle level, the categories of personal information the University collects, why it collects the information, how it uses and discloses the information, how it safeguards and retains the information, and how individuals may exercise access and correction rights.

Teams may refer individuals to the relevant notice where the proposed handling of personal information is clearly and specifically covered by it.

2. What the notices do not do

The existence of a general notice does not, by itself, authorise every collection, use or disclosure of personal information. The proposed handling must still be lawful, necessary for a University function, consistent with University policy and appropriately limited.

A separate or additional notice may be required where an activity involves information handling that is not adequately explained in the relevant lifecycle notice.

3. Before relying on a notice

Confirm each of the following:

- the person falls within the intended audience of the notice
- the category of personal or sensitive information is described
- the purpose for collection or use is described
- any proposed disclosure recipient and reason for disclosure are described
- the method of collection is consistent with the notice
- the activity does not introduce a materially different, unexpected or more intrusive use
- any legal, contractual, records, cybersecurity and information governance requirements have been addressed
- only the minimum information reasonably necessary will be handled

4. When an additional notice should be considered

- a new program, service, platform or technology collects information in a way individuals would not reasonably expect
- new categories of sensitive information are collected
- information is obtained from a new third-party source
- personal information will be used for a materially different purpose
- information will be disclosed to a recipient or category of recipient not described in the relevant lifecycle notice
- information will be published or made publicly available
- AI-enabled processing materially changes how information is analysed, generated or used
- participation is optional and consent may be the appropriate basis for the activity
- the activity affects a specific cohort and requires more tailored explanation

5. When a privacy impact assessment is required

The University requires a [privacy impact assessment](#) to be completed for any new or updated undertaking that involves the collection, use, disclosure, storage, access, retention or destruction of personal, health or sensitive information.

Completion of a privacy impact assessment helps determine whether the relevant lifecycle notice is sufficient, whether an additional notice or consent is needed, and what safeguards should be implemented before the undertaking proceeds or is updated.

6. Collection decision check

- Is the information reasonably necessary for a lawful University function or activity?
- Is the proposed collection directly from the individual unless another collection method is authorised?
- Has the individual been given an appropriate notice before or at the time of collection?
- Is the wording clear about whether providing the information is required or voluntary, and the consequences of not providing it?
- Are sensitive information requirements addressed?

7. Use decision check

- Is the proposed use the purpose for which the information was collected?
- If not, is the proposed use directly related to the original purpose and within reasonable expectations?
- Is the proposed use clearly described in the relevant notice?
- Will access be limited to staff who require the information for their role?
- Is a more limited or de-identified use reasonably available?

8. Disclosure decision check

- Is the recipient, or category of recipient, described in the relevant notice?
- Is the reason for disclosure described and connected to a University function or obligation?
- Is the disclosure required or authorised by law, or otherwise permitted under applicable privacy requirements?
- Will only the minimum necessary information be disclosed?
- Are appropriate contractual, security and recordkeeping controls in place?

9. If the activity is not clearly covered

Do not rely on the relevant notice unless the proposed collection, use or disclosure is clearly covered. Pause the activity and seek privacy advice. The [Privacy Office](#) can assist to determine whether an additional notice, consent, privacy impact assessment, contractual protection or other control is required.

10. Records and evidence

Teams should retain evidence of the notice provided and the version in effect, together with relevant approvals, privacy impact assessments, contracts, data-sharing documentation and decisions about the handling of personal information.

11. Contact and related documents

For privacy advice, contact privacy@westernsydney.edu.au.

- [Privacy Policy](#)
- [Privacy Management Plan](#)
- [Privacy Compliance website](#)