



# PRIVACY IN A NUTSHELL

Key elements of Privacy Compliance  
for all staff

**COLLECT**

**RESPECT**

**PROTECT**

*read more on the privacy pages at [www.westernsydney.edu.au/ougc/cpu](http://www.westernsydney.edu.au/ougc/cpu)*

# WHAT IS PRIVACY COMPLIANCE?

## The University's Privacy Compliance Office

- Sits within the Compliance Program Unit, and provides independent guidance, oversight, and assurance on the University's lawful management of personal information.
- We work in partnership with operational areas to support the identification, assessment, and management of privacy risks arising from the University's activities, systems, and services.

*Effective privacy management protects individuals and the University from legal, reputational, and operational risk.*

*It also supports trust, transparency, and responsible use of information across the University.*

## KEY PRINCIPLE

***Personal information must only be handled for a lawful purpose and protected from misuse, loss, or unauthorised access.***

# ROLES & RESPONSIBILITIES

## The Privacy Office

- Provides guidance on privacy obligations under applicable legislation
- Oversee and review Privacy Impact Assessments (PIAs) to independently identify privacy risks, and recommend mitigations prior to implementation
- Manage privacy breaches and complaints in accordance with legislative requirements
- Supports capability uplift through training and awareness



## Staff and Business Units

- Manage personal information within their operational area
- Collect only what is necessary for a lawful purpose
- Use and disclose information in accordance with defined purposes and requirements
- Ensure information is stored securely and access is restricted



**Operational areas are responsible for how personal information is handled within their functions.**

**The Privacy Office provides advice and oversight but does not make operational decisions on behalf of business units.**

# Privacy in Practice

## 1. Reporting Privacy Breaches

*When required*

- When an individual becomes aware of a suspected or actual incident involving personal information, including loss, unauthorised access, use, disclosure, or improper storage.

*What to do*

- Contain the issue immediately (e.g. restrict access, secure data)
- Notify the Privacy Office as soon as practicable
- Do not attempt to resolve or communicate externally without guidance

## 2. Completing Privacy Impact Assessments (PIAs)

*When required*

- New or changed systems, projects, or processes involving personal information *before launch*
- Changes to how personal information is collected, used, or disclosed

*What to do*

- Complete a Privacy Impact Assessment
- Assess risks and implement mitigation measures *before implementation*

## 3. Lawful Collection, Use and Transparency

*When required*

- A clear privacy collection notice at or before collection

*What to do*

- Ensure individuals understand why information is collected and how it will be used
- Keep notices accurate and aligned with actual practices

## Quick check (before you act)

- Is this necessary?
- Is the purpose clear and lawful?
- Is access controlled?
- Is this consistent with how the information was collected?
- **Contact [privacy@westernsydney.edu.au](mailto:privacy@westernsydney.edu.au)**

