




Residential Sales

Buyers Agents & Property Managers

Compulsory | Stock & Station – Strata – Commercial & additional topics

1



Fair Trading Requirements



Sales & Buyers Agents

- Anti-Money Laundering & Counter Terrorism
- Privacy Law Reforms
- Mitigating Risk & Managing Psychosocial Hazards
- Residential Tenancy Reforms

Property Managers

- Navigating NCAT
- Privacy Law Reforms
- Mitigating Risk & Managing Psychosocial Hazards
- Residential Tenancy Reforms

* Residential Sales – Buyers Agents – Property Managers – minimum 4 compulsory topics min 7 hours.
PLUS Class 1 agents must complete 5 hours with NSWFT

2



Fair Trading S&S Requirements

Stock & Station Agents

- Anti-Money Laundering & Counter Terrorism
- Privacy Law Reforms
- Mitigating Risk & Managing Psychosocial Hazards
- **Biosecurity, Disease Preparedness and Incident Response.**

Provider Options

ALPA Aust Livestock & Property Agents
<https://alpa.net.au/>

ACOP Aust College of Professionals
<https://acop.edu.au/>



* Stock & Station Agents – minimum 4 compulsory topics min 5 hours
PLUS Class 1 agents must complete 5 hours with NSWFT

3



Fair Trading Strata Requirements



Strata Agents

- Mitigating Risk & Managing Psychosocial Hazards
- **Regulatory change in Strata 2025**
- **Contracts & Contracting**

* TAFENSW Prescribed course – Commissions, disclosures and fiduciary duty (online course being developed)
All Strata Managing Agents are required to complete the course by 30 June 2026 and will be notified when this course is available

* Strata Agents – minimum 3 compulsory topics min 4 hours.
PLUS 1 hour TAFENSW – PLUS Class 1 agents must complete 5 hours with NSWFT

Provider Options

RETS Real Estate Training & Strata
<https://www.rets.com.au/>

ACOP Aust College of Professionals
<https://acop.edu.au/>

4



Fair Trading Requirements

Commercial Agents

- Anti-Money Laundering & Counter Terrorism
- Privacy Law Reforms
- Mitigating Risk & Managing Psychosocial Hazards
- **Retail & Commercial Leasing (incl Heads of Agreement)**



* Commercial Agents – minimum 4 compulsory topics min 5 hours.
PLUS Class 1 agents must complete 5 hours with NSWFT

5

Anti-Money Laundering & Counter Terrorism

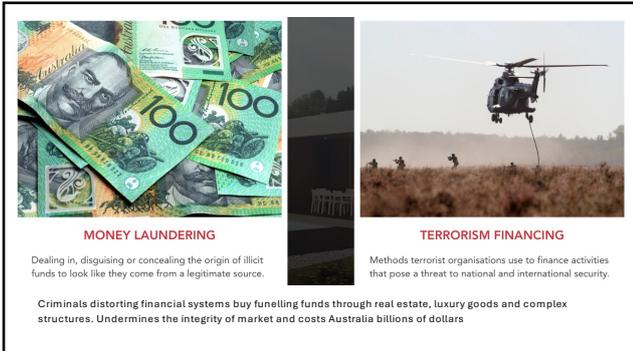


LEARNING OUTCOMES

By the end of this unit, you will be able to:

- 1 Understand the reforms to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- 2 Recognise the obligations property agents have around AML/CTF
- 3 Apply effective compliance practices that align with AML/CTF obligations
- 4 Identify potential suspicious activities and how to carry out reporting obligations
- 5 Understand the penalties and potential consequences for non-compliance with AML/CTF laws

6



MONEY LAUNDERING
Dealing in, disguising or concealing the origin of illicit funds to look like they come from a legitimate source.
Criminals distorting financial systems by funneling funds through real estate, luxury goods and complex structures. Undermines the integrity of market and costs Australia billions of dollars

TERRORISM FINANCING
Methods terrorist organisations use to finance activities that pose a threat to national and international security.

7

AUSTRAC
AUSTRAC is both the AML/CTF regulator and Australia's Financial Intelligence Unit (FIU).
New powers strengthen AUSTRAC's ability to:

- Examine entities for enforcement and court proceedings
- Request documents to support intelligence and regulatory functions
- Enable voluntary cooperation without legal risk (e.g. Fintel Alliance)



8

DESIGNATED SERVICES
The Amendment Act will extend AML/CTF regulation to real estate professionals that provide the following services:

- Real estate agents and businesses that broker the sale, purchase, or transfer of property on behalf of clients, as part of their business operations.
- Property developers and similar businesses selling or transferring real estate directly without using an independent agent.
- The services will NOT capture:
 - Residential tenancy agreements
 - Property management
 - Leasing of commercial real estate
 - Auctioneer services

9

YOUR ROLE IN IDENTIFYING SUSPICIOUS TRANSACTIONS

1 IDENTIFY RED FLAGS

- Be alert to unusual patterns
- Look for behaviours that don't add up
- Question involvement of third parties
- Flag unusual payment methods

10

RED FLAG EXAMPLES

Real Estate Sector

Use of complex loans or finance	Customers selling for less than the market value
Manipulation of a property's valuation or appraisal	Unusual involvement of third parties
Use of monetary instruments	Lack of transparency regarding a company's structure in the public domain
Use of investment schemes	Unnecessarily complex transactions
Properties being bought and sold in quick succession	

11

RED FLAG EXAMPLES

Clients/Customers

Significant and unexplained geographical distance between your premises and the location of the client	Sudden activity from a previously dormant client
Customer purchases properties at significantly higher or lower prices than the market	Client alters a transaction after being asked for further information
Unusual or complex business structures	Client appears nervous or defensive, especially when questioned
Difficulties in identifying the beneficial owners	Client refuses to identify the source of funds
Customer is reluctant to provide all CDD information	Client wishes to purchase property in someone else's name
Client's access to funds does not match their profile	Client purchases property without viewing it
Client shows little interest in price	

12

YOUR ROLE IN IDENTIFYING SUSPICIOUS TRANSACTIONS

- 1
- 2
- 3

TAKE APPROPRIATE ACTION



- Record the details of the transaction and customer behaviour
- Report to your compliance officer or Money Laundering Reporting Officer (MLRO)
- Lodge a Suspicious Matter Report (SMR) with AUSTRAC

13

AML/CTF RULES THAT APPLY TO THE PROPERTY INDUSTRY



- Allocate compliance officer (Part 8.5)
- Create risk assessment process (Rules 8.1.4, 8.1.5)
- Develop risk awareness program (Part 8.2)
- Register with AUSTRAC (ss 516, 517, 740)
- Develop employee due diligence program (Part 8.3)
- Collect and verify KYC information (ss 52, 55)
- Perform ongoing CDD and transaction monitoring (Parts 15.2-15.11)
- Keep records (Chapter 20)
- Report to AUSTRAC (Part 8.6)
- Conduct independent review (Part 8.4)
- Respond to AUSTRAC (Part 8.7)

14

YOUR ROLE IN IDENTIFYING SUSPICIOUS TRANSACTIONS

- 1
- 2
- 3

DON'T TIP OFF

Do not inform the customer you're making a report - this is a criminal offence



15

There are **6 key obligations** for reporting entities:

- Enrolment with AUSTRAC
- AML/CTF Program
- Initial Customer Due Diligence (CDD)
- Ongoing Customer Due Diligence
- Reporting
- Record Keeping

COMPLIANCE REQUIREMENTS **FOR REAL ESTATE AGENTS**

16

If your business provides **designated services**, you must enrol with AUSTRAC.

You'll receive access to **AUSTRAC Online** to:

- Submit transaction/compliance reports
- View/update your business details

17

Key AUSTRAC enrolment dates:

- 31 March 2026: Enrolment with AUSTRAC opens
- 1 July 2026: New AML/CTF obligations commence
- 29 July 2026: Final date to complete enrolment with AUSTRAC

1 Enrolment with AUSTRAC

2 AML/CTF Program

An AML/CTF Program outlines:

- How your business identifies and manages ML/CF risks
- Policies and procedures to comply with legal obligations

The program must include:

- Risk assessments
- Internal controls

18

3 Initial Customer Due Diligence (CDD)

Verify the identity of all customers before providing services by collecting KYC (Know Your Customer) information, such as:

- Individuals** Full name, DOB, Address
- Businesses** Company name, ABN, Directors/Shareholders

CDD and KYC help identify customers, assess risk, and prevent misuse of services for ML/TF. It must be applied before and during a business relationship, based on the customer's risk level.

Assess risk level and apply:

- Standard CDD** (Low risk customers)
- Enhanced CDD** (High risk customers)
 - Apply when:
 - Customer is a Politically Exposed Person (PEP)
 - Customer is a high-risk jurisdiction
 - Customer is a natural person who is a PEP
 - Customer is a high-risk individual
 - Customer is a high-risk business
- Simplified CDD** (Low risk customers)
 - Apply when:
 - Customer is a low-risk jurisdiction
 - Customer is a low-risk individual
 - Customer is a low-risk business

19

5 Reporting **4 Ongoing Customer Due Diligence (CDD)**

Report to AUSTRAC via AUSTRAC Online when:

- A Threshold Transaction** involves \$10,000 or more in cash
- There are reasonable grounds for suspicion (eg. See identify criminal activity)
- These reports include SMs and TTRs

SMR suspicious matter report - TTR transfer of physical currency (cash) of AS\$10,000 or more

- Monitor customers continuously for suspicious or unusual activity
- Keep KYC information updated and respond to changes in customer risk
- Level of monitoring should match the level of risk
- Helps detect potential criminal misuse over time

20

6 Record Keeping

- Keep clear records of:
 - Customer ID and due diligence
 - Services provided
 - Steps taken to meet AML/CTF obligations
- No need to keep copies of ID documents - just record the information used
- Must comply with Privacy Act 1988 when storing customer data

FURTHER GUIDANCE AND RESOURCES
where further guidance and training about new obligations on real estate agents in relation to AML/CTF can be found

- The Attorney-General's Department website - ag.gov.au
- AUSTRAC's official website - austrac.gov.au
- AUSTRAC's eLearning platform - elearn.austrac.gov.au

21

MODULE 3

EFFECTIVE COMPLIANCE PRACTICES

22

APPLYING A RISK-BASED APPROACH TO ML/TF RISKS

- Identify and assess risks** - that your business faces from ML/TF
- Apply controls** - proportionate to the level of risk
- Review and update** - your risk assessment to address threats
- Implement systems** - controls and staff training to manage risks
- Document risk approach** - and monitor its effectiveness

23

INTERNAL AML/CTF POLICIES AND PROCEDURES

- 1. Appoint a Compliance Officer**
 - Must be a fit and proper person at management level
 - Must have access to staff, systems, and authority to manage AML/CTF compliance
 - Sole traders may seek advice but remain responsible for compliance
- 2. Identify Verification Procedures**
 - Follow NSW Supervision Guidelines to meet AML/CTF CDD obligations
 - Verify identity using:
 - 1 Primary document (e.g. driver's licence)
 - 2 Secondary documents (e.g. medicare)
 - Verification can be done in person, electronically, or via video call

24

RECORD-KEEPING AND ONGOING COMPLIANCE

You must keep accurate records of:

- Transactions
- Customer identification (KYC/CDD)
- Your AML/CTF program

Proper record-keeping helps prove compliance and supports investigations if criminal activity occurs

Storage Requirements

- Records must be secure, retrievable and auditable
- Can be kept electronically or in hard copy, on-site or off-site

Timeframes

- Records must be kept for 7 years
- Remitters and digital currency exchanges must retain records until deregistration

25

SHARED COMPLIANCE VIA GROUP AML/CTF PROGRAMS

Real estate franchises and related businesses can form a **Designated Business Group (DBG)** to share AML/CTF compliance responsibilities.

Benefits of a DBG

- Share costs and admin for AML/CTF programs, record-keeping, and compliance tasks.
- A lead reporting entity can manage obligations on behalf of the group.

Eligibility Examples

- Joint ventures
- Related companies
- Franchise networks
- Certain legal or accounting practices

Setup Requirements

- Must agree in writing
- Appoint a nominated contact officer
- Submit Form 1 (for each member) and Form 2 (to form the DBG) via AUSTRAC Online

26

SUSPICIOUS MATTER REPORTS

If you detect a suspicious transaction or activity that may relate to crime, you must submit a suspicious matter report (SMR) in accordance to section 41 of the AML/CTF Act.

You must submit an SMR to AUSTRAC within:

- **24 hours** if your suspicion is related to terrorism financing
- **3 business days** if your suspicion is related to anything other than terrorism financing (such as money laundering or tax evasion)

SUSPICIOUS MATTER REPORTS

SMRs must include:

- Whether the individual is a customer of your business
- Whether they have asked you to provide a service that you normally provide
- Whether they enquired if you would be prepared to provide that service
- Whether you have commenced providing, or plan to provide, that service
- A description of the suspicious matter with reference to section 41 of the act
- A description of the service to which the suspicious matter relates
- A description of the grounds for suspicion
- Retain a copy of your AML/CTF program for seven years after it has ceased to have effect - this includes where an old program has been superseded

27

SUSPICIOUS MATTER REPORTS

If you have submitted an SMR, or are required to do so, you must not disclose this information to anyone (except an AUSTRAC-entrusted person) or disclose information that could determine that you have submitted an SMR.

Exceptions to this include:

- Providing legal or financial advice to a client
- Sharing information within a designated business group
- Engaging with law enforcement and regulatory agencies
- Disclosing to a court or tribunal for proceedings brought under the AML/CTF Act

THRESHOLD TRANSACTION REPORTS

You must submit a Threshold transaction report (TTR) to AUSTRAC if you have provided, or plan to provide a service to a customer that involves a threshold transaction.

Threshold transaction involves the transfer of **\$10,000 or more** in physical currency.

The report must be sent to AUSTRAC **within 10 days** of receiving the funds.

28

ANNUAL REPORTING OBLIGATIONS

In accordance with section 47 of the AML/CTF Act, you must lodge a report with AUSTRAC relating to your compliance.

Only **listed administrators** of your business can submit the reports. The annual compliance report must:

- Demonstrate that you are meeting your obligations
- Be lodged by **31 March** for the prior 12-month period of 1 January to 31 December

By what date must your annual AML/CTF compliance report be submitted?

31 December

1 July

31 March

Submit

• Your name will be shared

29

POTENTIAL CONSEQUENCES OF NON-COMPLIANCE WITH AML/CTF LAWS

If you don't meet your obligations under AML/CTF law, AUSTRAC can take steps to enforce your compliance and/or seek a penalty.

Enforcement actions available to AUSTRAC are:

- Civil penalty orders – up to 20,000 penalty units, or up to 100,000 penalty units for a body corporate
- Enforceable undertakings
- Infringement notices
- Remedial directions

AUSTRAC can also issue a **written notice** requiring you to appoint an external auditor or to undertake a ML/TF financing risk assessment.

30



REAL ESTATE
CFR 2025-2026
RESIDENTIAL SALESPERSONS
COMMERCIAL REAL ESTATE AGENTS

PRIVACY LAW REFORMS

LEARNING OUTCOMES

By the end of this unit, you will be able to:

- 1 Describe the amendments to the Privacy Act 1988 and their implications for the strata and property services sector.
- 2 Identify and recognise the Australian Privacy Principles (APPs) and agency obligations around the use of personal and sensitive information.
- 3 Apply strategies to protect personal information and ensure compliance with updated breach notification requirements.
- 4 Recognise specific privacy obligations and apply appropriate disclosure procedures when handling personal information.
- 5 Understand data breach reporting requirements and review agency policies to ensure ongoing compliance with privacy laws.

31



MODULE 1
KEY CHANGES TO THE PRIVACY ACT 1988

WHAT ARE THE CHANGES?

- 1 **Cross-border disclosure of personal information**
New regulations identify other countries' privacy policies where data is sent.
- 2 **Eligible data breaches**
The scope for an eligible data breach has been widened.
- 3 **Automated decisions**
New transparency obligations when using automated decisions.
- 4 **Civil penalties for serious interference with privacy**
New penalties for providing false or misleading information or data breach notifications or other serious breaches.

32

CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

A property manager in NSW is managing a rental property for a landlord who lives in the UK. The landlord requests that copies of tenant applications, lease agreements, and maintenance reports be emailed directly to them for approval.

Steps to take to ensure privacy:

- 🔒 Explaining the Australian privacy obligations to the landlord
- 📄 Written agreement that the landlord understands their responsibilities

CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

This new regulation will identify if another country has similar protections for data as the Australian Privacy Principles (APPs) and if effective enforcements exist.

i This recognises that the laws of a country may vary in relation to certain entities or information

33

ELIGIBLE DATA BREACHES

The definition of a data breach now includes clearer criteria on what constitutes serious harm to individuals.

Serious harm is understood to include:

- 🚫 Identity fraud
- 🚫 Reputational damage
- 🚫 Blackmail
- 🚫 Significant financial loss
- 🚫 Emotional distress

ELIGIBLE DATA BREACHES

A rental application including a tenant's passport and bank details is mistakenly emailed to the wrong landlord.

AUTOMATED DECISIONS

New transparency obligations require organisations to update their privacy policies to disclose when decisions are made using automated processes.

i This change comes as AI technology becomes more prevalent causing more privacy concerns.

AUTOMATED DECISIONS

A real estate agency uses a property management platform that automatically scores and ranks tenant applications based on income, rental history, and background checks. This then determines if the application is approved or rejected.

34

AUTOMATED DECISIONS

Does your agency currently use any form of automated decision-making?

Yes

No

Not sure

🟢 Your name will be shared 10 votes

Examples:

- Digital ID verification and background checks
- CRM emailing
- Tenant application scoring
- AI chatbots



35

CIVIL PENALTY PROVISIONS FOR SERIOUS INTERFERENCE WITH PRIVACY OF AN INDIVIDUAL

An agent shares a tenants personal information including their mobile number and lease agreement with a plumber doing non-urgent repairs, without informing the tenant or getting their permission.

The plumber later contacts the tenant directly and uses their personal details for unrelated marketing.

CIVIL PENALTY PROVISIONS FOR SERIOUS INTERFERENCE WITH PRIVACY OF AN INDIVIDUAL

The new statutory tort will allow individuals to take action against others for a broader range of serious invasions of privacy, including physical privacy and misuse of information.

Maximum penalties include:

- For an individual: \$2,500,000
- For a body corporate: \$50,000,000 or three times the value of the benefit obtained by the body corporate that is reasonably attributable to the conduct; or 30% of the body corporate's adjusted turnover

36

THE AUSTRALIAN PRIVACY PRINCIPLES (APPS)

There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- The collection, use and disclosure of personal information
- An organisation or agency's governance and accountability
- Integrity and correction of personal information
- The rights of individuals to access their personal information

The APPs give organisations and agencies flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals.

37

THE AUSTRALIAN PRIVACY PRINCIPLES (APPS)

APP 01 Open and transparent management of personal information.	APP 08 Cross-border disclosure of personal information
APP 02 Anonymity and pseudonymity	APP 09 Adoption, use or disclosure of government related identifiers
APP 03 Collection of solicited personal information	APP 10 Quality of personal information
APP 04 Dealing with unsolicited personal information	APP 11 Security of personal information
APP 05 Notification of the collection of personal information	APP 12 Access to personal information
APP 06 Use or disclosure of personal information	APP 13 Correction of personal information
APP 07 Direct marketing	

38

HANDLING INFORMATION ABOUT CUSTOMERS

Agencies deal with a great deal of Client Information (Data) on a day-to-day basis. This includes:

- Tenant application information
- Agency agreements
- Contracts for sale
- Residential tenancy agreements
- Other lease agreements such as retail leases
- Id check information
- Customer marketing data
- Tenant data such as tenant history

Agencies must utilise data only relevant to business transactions and business processes that are being carried out according to Client instructions and the APPs.

For example:

- USING CONTACT INFORMATION TO CONTACT THEIR CLIENTS
- USING FINANCIAL INFORMATION TO MANAGE THEIR CLIENTS' DEPOSITS AND PAYMENTS
- USING CLIENT PREFERENCE AND PROFILES TO IDENTIFY PROPERTIES
- USING CLIENT INFORMATION TO COMPLETE AGENCY AGREEMENTS OR LEASE DOCUMENTS

39

APP 11: Security of personal information

An agency stores tenancy applications in a secure cloud-based system with restricted user access and automatic backups, instead of in unlocking filing cabinets.

APP 6: Use of disclosure of personal information

An agent receives a tenant's contact number during their lease and does not share it with third-party tradespeople unless the tenant agrees or it is required to complete urgent repairs.

An acknowledgement in the lease stating that the number can be provided will counteract this.

APP 3: Personal information must only be collected by lawful and fair means

A property manager collects a tenant's employment history and proof of income when processing a rental application but does not request unnecessary personal details like the applicants relationship status or religion.

APP 5: Notification of the collection of personal information

A sales agent provides a Privacy Collection Notice on the open home sign-in sheet, letting potential buyers know that their contact details will be used for follow-up marketing and will be stored securely.

An agent also must not use or disclose confidential information (including personal information) unless the client or customer authorises this use, or it is otherwise required by law.

40

BEST PRACTICES FOR DATA PROTECTION AND SECURITY

DATA BREACH NOTIFICATION REQUIREMENTS

A data breach occurs when personal information is accessed, disclosed without authorisation, or is lost. When this happens an organisation or agency must tell the OAIC of the breach and notify the affected individuals.

41

THE ACTIONS TAKEN FOLLOWING A DATA BREACH SHOULD FOLLOW THESE FOUR KEY STEPS:

- Contain**
the breach to prevent any further compromise of personal information.
- Assess**
the data breach by gathering the facts and evaluating the risks.
- Notify**
individuals and the Commissioner if required.
- Review**
the incident and consider what actions can be taken to prevent future breaches

42

PRIVACY IN DAILY OPERATIONS

PRIVACY CONSIDERATIONS FOR SPECIFIC AGENCY TYPES

! Not limited to these considerations

Residential Real Estate Salepeople	Residential Real Estate Buyers Agents
Must not disclose sensitive client information unless authorised or legally required.	Must maintain strict confidentiality around the buyer's financial capacity, urgency, or motivations.
Must notify vendors and buyers of how their personal information is collected, stored and shared.	Inform clients of how their information will be used and stored.
Must not use personal data for marketing beyond that original purpose unless the individual has given consent or has an option to opt-out.	Must lawfully collect information about sellers, listings, and market prospects. Any third-party data must be obtained using fair and non-intrusive means.
Personal information used in listing, promoting, and negotiating sales must be accurate and up-to-date.	If buyer info is shared with mortgage brokers, conveyancers, or builders, disclosure must be authorised or legally permitted.

43

PRIVACY CONSIDERATIONS FOR SPECIFIC AGENCY TYPES

PRIVACY CONSIDERATIONS FOR SPECIFIC AGENCY TYPES

! Not limited to these considerations

Residential Property Managers	Commercial Real Estate Agents
Handle large volumes of tenant personal information which must be stored securely and limit access to authorised personnel only.	Often manage transactions involving business clients which must be handled confidentially.
Must inform tenants and landlords how their personal data will be used and for how long it will be kept.	Must ensure fair collection of business leads and avoid using intrusive methods or misusing third-party data lists.
Any sharing of data with third parties must be disclosed and limited to what is necessary.	If client info is collected during property enquiries, agents must notify clients how their data will be used.
Must have data destruction protocols once tenancy ends and data is no longer needed.	Must ensure that personal or business contact data is kept secure, especially when handled by a team or via a CRM system.

44

DISCLOSURE AND CONSENT PROCEDURES

APP 5
APP 6
Consent

Notification of collection of personal information
The matters that agents must notify individuals of include:

- The purposes of collection
- Who the information may be disclosed to
- How the individual can access and correct the information or complain about a breach

45

Use or disclosure of personal information

Reasons why agents collect personal information may include:

- To provide clients with the best possible experiences
- To enable statutory information to be collected
- To enable the accurate processing of any monies that are held on the client's behalf
- To ensure that properties are legitimately owned
- To identify parties to transactions accurately to remove the risk of fraud

What is Consent?
The four key elements of consent are:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific
- The individual has the capacity to understand and communicate their consent

46

MODULE 5

NEW REPORTING AND ACCOUNTABILITY REQUIREMENTS

47

MANDATORY REPORTING OBLIGATIONS FOR DATA BREACHES

If an agency has detected a data breach, then it must inform the individual concerned via email, telephone or text message.

The notification should include:

- The organisation or agency's name and contact details
- The kinds of personal information involved in the breach
- A description of the data breach
- Recommendations for the steps you can take in response

If an agency can't directly contact affected individuals about a breach, it must publish the notification on its website and actively promote it, such as via social media or news outlets. The breach should be reported to the OAIC using their online data breach form.

48

OAIC DATA BREACH FORM

Report your data breach
This form is for use by the OAIC to assist you in reporting a data breach. It is not a legal document.

Organisation details
Name: _____
ABN: _____
ACN: _____
Postal address: _____
City: _____ State: _____
Postal code: _____
Phone: _____
Email: _____

Details of the data breach
Date of breach: _____
Time of breach: _____
Type of breach: _____
Number of records affected: _____
Description of the data breach: _____
How the breach occurred: _____
How the breach was discovered: _____
How the breach was contained: _____

Part two - Additional information
How you plan to respond: _____
How you plan to notify affected individuals: _____
How you plan to notify the OAIC: _____
How you plan to prevent a recurrence: _____
How you plan to improve your data security: _____

49

REVIEWING POLICIES AND PROCEDURES TO MAINTAIN COMPLIANCE WITH EVOLVING PRIVACY LAWS

Entities are encouraged to regularly review and update their privacy policies, internal practices, and training programs.

The OAIC has an Interactive Privacy Management Plan that agencies can use to ensure this obligation occurs.

50

Interactive Privacy Management Plan

OAIC Plan explained
https://www.oaic.gov.au/data/assets/pdf_file/0005/1301/interactive-mpm-explained.pdf

Introduction
The Interactive Privacy Management Plan (IPMP) has been developed by the Office of the Australian Information Commissioner (OAIC) to assist public sector agencies comply with the requirements of the Australian Government Privacy Code (AGPC) and their Australian Privacy Principles (APPs), and to ensure the arrangements which will deliver the most value to them.

How to use
Before you begin
The OAIC has developed a public sector Interactive Privacy Management Plan (IPMP) which is designed to help agencies manage their privacy risks. It is assumed that you have read the OAIC's Privacy Code and completed any preliminary steps that it recommends prior to starting with the Interactive IPMP.

51

MANAGING PSYCHOSOCIAL HAZARDS IN THE WORKPLACE

LEARNING OUTCOMES
By the end of this unit, you will be able to:

- 1 Understand legal responsibilities and guidance
- 2 Recognise and assess psychosocial hazards
- 3 Apply risk management processes to psychosocial hazards
- 4 Promote a mentally healthy and respectful workplace

52

LEGISLATIVE DUTIES

What is a Psychosocial Hazard?

A psychosocial hazard is anything at work that could harm someone's mental health.

These hazards often lead to stress, which can cause:

- Psychological harm
- Physical harm

Stress itself is not an injury. But if workers are stressed often, over a long time, or the level of stress is high, it can cause harm.

53

LEGAL DUTIES UNDER THE WHS ACT 2011

PCBU	Officer	Workers
Section 19 – Primary Duty of Care		
PCBU duties include:		
<ul style="list-style-type: none"> Identify foreseeable hazards Eliminate or minimise psychosocial risks Maintain and review controls Consider all relevant workplace factors 		

PCBU - Person Conducting a Business or Undertaking. - replacing the term "employer"

54

PCBU **Officer** **Workers**

Section 27 – Duty of Officers
Officer duties include:

- Keep up-to-date with WHS matters
- Understand business operations and risks
- Ensure proper systems and resources are in place
- Monitor and verify effectiveness of controls

55

PCBU **Officer** **Workers**

Section 28 – Duty of Workers
While at work, a worker must:

- Take care of own and others' health and safety
- Follow WHS instructions and procedures
- Report issues and cooperate with policies

56

CODE OF PRACTICE

The Code of Practice provides practical guidance on managing psychosocial hazards at work and is approved under section 274 of the Work Health and Safety Act 2011.

What harm can psychosocial hazards cause?
Psychosocial hazards can cause psychological and physical harm.

Why are psychosocial injuries a major concern?
On average, work-related psychological injuries have longer recovery times, higher costs, and require more time away from work.

Why should we manage psychosocial risks?
Managing these risks not only protects workers, it also decreases the disruption associated with staff turnover and absenteeism, and may improve organisational performance and productivity.

57

RECOGNISING PSYCHOSOCIAL HAZARDS IN THE WORKPLACE

Psychosocial vs Other WHS Risks

While, psychosocial risks primarily affect mental and emotional wellbeing, other WHS risks involve **physical harm**.

Common WHS hazards that involve physical harm include:

- Physical Hazards**: Slips, trips, and falls; Machinery and equipment
- Chemical Hazards**: Exposure to toxic substances and proper handling and storage
- Ergonomic Hazards**: Poor workstation setup and repetitive strain injuries

58

COMMON PSYCHOSOCIAL HAZARDS

JOB DEMANDS & CONTROL	High workloads, limited autonomy, tight deadlines
POOR SUPPORT & ROLE CLARITY	Inadequate guidance and resources, changing job expectations
POOR ORGANISATIONAL PRACTICES	Lack of recognition or fair treatment, poor change management
REMOTE & ISOLATED WORK	Working alone, after hours, or far from help
UNSAFE PHYSICAL OR SOCIAL ENVIRONMENT	Unsafe or hostile workspaces, conflict with clients or colleagues

59

HOW THESE HAZARDS SHOW UP IN AGENCY PRACTICE

CLIENT AGGRESSION	Tenants yelling at property managers during evictions
ISOLATED WORK	Agents conducting open homes alone or at night
HIGH JOB DEMANDS	Sales agents managing multiple listings under tight deadlines
ROLE AMBIGUITY	New staff unsure who handles repairs vs. lease renewals
POOR WORKPLACE CULTURE	Gossip, exclusion, or unresolved team tension
HARASSMENT	Unwanted comments from clients during inspections

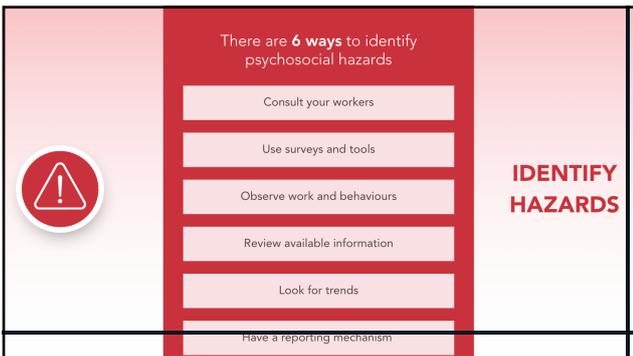
60



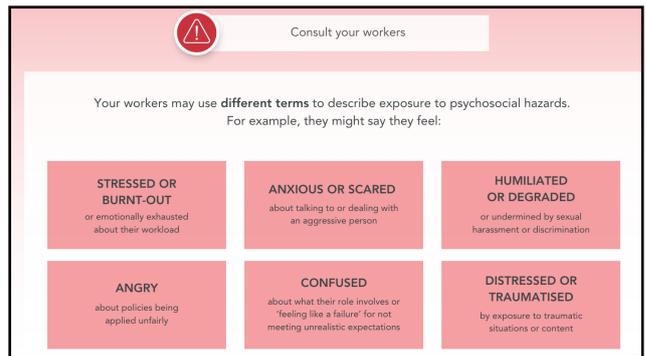
61



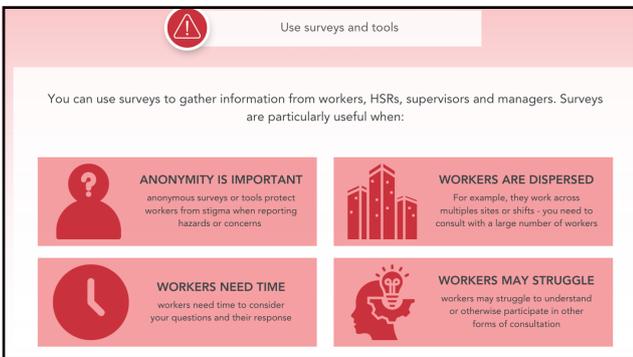
62



63



64



65



66

Have a reporting mechanism

It is important for hazards reported by workers be **taken seriously**.
Workers can be encouraged to report hazards by:

treating all reports of psychosocial hazards seriously and appropriately	using agreed mechanisms , such as HSRs who can raise safety concerns for workers anonymously	regularly discussing psychosocial hazards at team meetings	providing workers with a range of accessible and user-friendly ways to make a report
making it clear that victimising those who make reports will not be tolerated	training key workers (e.g. supervisors, managers, contact persons and HSR)	ensuring processes and systems for reporting and responding to complaints	acting decisively to control the risks your workers identify

67

Have a reporting mechanism

Workers might not report psychosocial hazards because they:

- feel like it's 'part of the job'
- believe it's not serious enough
- feel they do not have time
- think reports will be ignored
- fear they will be blamed
- do not know how to report

68

How to assess psychosocial risks

Once you have identified all the hazards you should assess the risk. To do this, consider:

DURATION	How long is the worker exposed to the hazards or risks?
FREQUENCY	How often is the worker exposed to the hazards or risks?
SEVERITY	How severe are the hazards and the workers' exposures?

69

The best combination of control measures will be tailored to your organisation's size, type and work activities to manage risks during both everyday operations and emergencies.

To determine what is reasonably practicable to manage psychosocial risks:

- Identify as many control measures as you can
- Consider which controls are most effective
- Consider which controls are reasonably practicable

CONTROL HAZARDS

70

Identify control measures

To identify what can be done you should, in consultation with your workers, identify as many possible control measures as you can.

This gives you the greatest scope to choose and apply the most effective control measures to eliminate or minimise risks.

Consultation with workers will assist you to identify control measures you might not otherwise think of.

71

ELIMINATION	Stop conducting after-hours open homes alone to eliminate risk of client aggression or isolation.
SUBSTITUTION	Replace high-pressure sales targets with team-based goals to reduce individual stress and promote collaboration.
ISOLATION	Use virtual property tours to avoid unsafe in-person meetings; conduct open homes in pairs; set up secure drop boxes for keys/documents.
ENGINEERING	Install CCTV cameras and secure access systems in offices or high-risk areas; use high counters or glass screens in reception areas.
ADMIN	Set realistic deadlines and flexible working arrangements; provide mental health training and clear reporting protocols.
PPE	Use noise-cancelling headsets for staff working in open-plan offices to reduce noise exposure, supporting focus and mental wellbeing.

72

 Eliminating the risks

Minimising the risks can be achieved by changing the:


 design of work


 systems of work


 work environment


 workplace interactions


 objects or tools used in the task

73



Reviewing control measures should be **done regularly** and is required:

- when the control measure is not eliminating or minimising the risks
- before a change at the workplace that is likely to give rise to new health and safety risks
- if a new hazard or risk is identified
- if the results of consultation indicate a review is necessary
- if an HSR requests a review

REVIEW
HAZARDS

74

Common review methods include:


 Inspecting the workplace


 Consultation


 Analysing records and data

75

REDUCING RISK EXPOSURE

PHYSICAL WORK ENVIRONMENT AND SECURITY

- Security guards, video surveillance, alarms
- Well-maintained vehicles with safety features
- Controlled access
- Good lighting and visibility
- Safe layouts preventing entrapment, secure objects

REDUCING RISK EXPOSURE

INFORMATION, TRAINING AND POLICIES

- Train workers in conflict resolution, de-escalation and reporting
- Clear behaviour standards, zero tolerance policies
- Support for workers making reports; consistent handling of incidents
- Foster positive culture, address power imbalances and diversity

REDUCING RISK EXPOSURE

SAFE WORK SYSTEMS AND PROCEDURES

- Communication - regular check-ins and clear client conduct policies
- Procedures - Ban/limit poorly behaved clients
- Avoid lone work where possible, provide supervision and support
- Incident reporting, escalation protocols, risk assessments

76

MODULE 4

PROMOTING A MENTALLY
HEALTHY WORKPLACE CULTURE

77

SET THE STANDARD

WORKPLACE BEHAVIOURS

Set Clear Behaviour Standards
Define acceptable conduct through a Code of Conduct or policy; apply to all work-related actions.

Implement Bullying Policy
Written, worker-consulted policy with bullying definition, reporting process, and consequences.

Good Management Practices
Train leaders, support staff, encourage teamwork, clearly communicate expectations, and act promptly on issues.



78

TECHNIQUES FOR INITIATING SUPPORTIVE CONVERSATIONS

- A** Approach, assess and assist
- L** Listen and communicate
- G** Give support and information
- E** Encourage professional help
- E** Encourage other supports

79

ALGEE METHOD SCENARIO

Sophie is a property manager at a busy real estate agency. Lately, her colleague Daniel has seemed **withdrawn, easily irritated**, and has started **missing deadlines**, which is something very out of character for him.

- A** Approach, Assess and Assist
Sophie checks in privately - "Are you okay? You seem a bit off lately."
- L** Listen and Communicate
Daniel shares he's overwhelmed. Sophie listens calmly, without judgement.
- G** Give Support and Information
Sophie reassures him and shares that help is available.
- E** Encourage Professional Help
Suggests speaking to the EAP or a GP for support.
- E** Encourage Other Supports
Asks if he has trusted people to talk to and offers help with workload.

80

**REPORTING PSYCHOSOCIAL HAZARDS
WHS STEPS**

- 1 Confirm the Issue**
Check if behaviour meets the definition of a psychosocial hazard (refer to NSW Code of Practice)
- 2 Try to Resolve Internally**
• Speak to supervisor, manager, HSR or Union Rep
• Use your workplace's reporting procedures
• Report early
- 3 If Unresolved, Escalate**
• Contact SafeWork NSW if the issue isn't resolved
• Submit a Request for Service Form (online or by phone)
- 4 Provide Clear Evidence**
Include behaviours, dates, locations, witnesses, and documents (e.g. emails, diary entries)

81

safe work australia
FURTHER GUIDANCE AND RESOURCES

- Psychosocial Hazards**
<https://www.safeworkaustralia.gov.au/safety-topics/managing-health-and-safety/mental-health/psychosocial-hazards>
- Managing Psychosocial Risks at Work**
<https://www.safeworkaustralia.gov.au/media-centre/news/managing-psychosocialrisks-work>
- Mental Health Resources**
<https://www.safeworkaustralia.gov.au/safety-topics/managing-health-and-safety/mental-health/resources>

82

Residential Tenancy Reforms and Navigating NCAT coming up

83