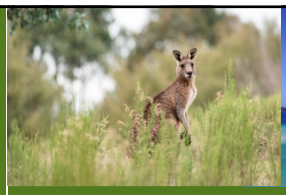
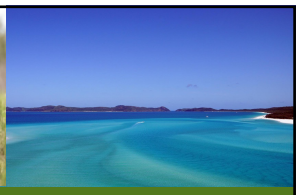



2022-23 Compulsory CPD

Cyber Security & Fraud – Underquoting - Privacy

Evelyn Olivares
0418 403 227

Real Estate Training Solutions RTO#90897
CPD period 23 Mar 22 to 22 Mar 23

realfocus development partners

RETS Real Estate Training Solutions

1

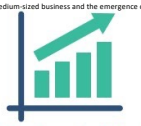
Topic 1 – Cyber Security & Fraud

realfocus development partners

2

Cybercrime

Image Source: 'Cyber Scare- A look at small to medium-sized business and the emergence of cybercrime in Australia'.



The cost of cybercrime to businesses in Australia is rising exponentially, costing Australians an estimated **$1 billion** each year.

Cybercrime costs businesses globally more than **$3 trillion** annually and it is anticipated that by 2021 this will exceed $6 trillion.[10]

realfocus development partners

3

What is Cyber crime and Fraud?

What is 'cybercrime'?

'Cybercrime1' can be defined as '***dishonest or criminal activity online*** or by phone. Cybercrime can include deceptive conduct like ***malicious software*** or ***viruses***, ***online or phone scams***, ***theft of critical business information***, fake overpayments, ***fake invoicing or hacking*** a business to ***obtain a customer's details or access to a supplier's network'***

What is 'fraud'?

Fraud involves ***dishonestly obtaining a benefit***, or ***causing a loss***, by ***deception*** or other means'.

realfocus development partners

4

Why the property industry is at particular risk to cybercrime and fraud

- the agent/client relationship is a fiduciary one (i.e. a relationship of trust)
- property agents are entrusted with their client's and customer's personal information, which in the wrong hands, ***can lead to identity theft***
- businesses ***store information in the cloud***, to make it available to stakeholders, but this ***also makes it available to hackers***
- property agents work with a variety of clients and customers, and each transaction such as a ***sale may involve several parties***, providing ample opportunity for an internal or external party to ***wreak havoc***
- large amounts of money and stressful emotions are involved in many property transactions, making parties more open to being scammed
- property agents often work long hours and ***tired/stressed people can make mistakes, i.e. 'human error'.***

realfocus development partners

5

BEC scams = 'business email compromise'

A ***BEC scam***, cybercriminals ***pose as a legitimate business*** to send ***fraudulent emails*** to their customers or clients. ***In a property-related BEC, cybercriminals unlawfully gain access to emails or impersonate businesses to deceive individuals attempting to buy, sell or lease property.***

Cybercriminals will impersonate parties to a property transaction (such as real estate agents or conveyancers) ***and insert illegitimate bank details*** for ***settlement*** or ***rental payments***.

Victims assume this request is legitimate and will unknowingly send -payment to the cybercriminal's bank account. ***Successful BECs can go unnoticed for weeks*** until businesses follow up on a missing payment.

Source: https://www.cyber.gov.au/acsc/view-all-content/alerts/property-related-business-email- compromise-scams-rising-australia

realfocus development partners

6

BEC scams = 'business email compromise'

These ***fraudulent emails may come from hacked email accounts***, or cybercriminals ***might register domain names*** that are ***similar*** to ***legitimate companies*** (typically by swapping letters or adding additional characters). They might also create ***email addresses with Gmail***, ***Yahoo*** or ***Outlook*** that use the legitimate business name.

At a quick glance, an ***email*** address may ***look legitimate*** when it is actually being operated by a cybercriminal.

Cybercriminals are ***targeting all parties involved in the real estate sector***, with a particular focus on ***impersonating conveyancing lawyers*** and communicating with their clients.

Cybercriminals are also singling out mortgage lenders in order to intercept property settlements.

Source: https://www.cyber.gov.au/acsc/view-all-content/alerts/property-related-business-email- compromise-scams-rising-australia

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

7

Email Spoofing

E-mail '***spoofing***' refers to using ***e-mail software*** to make it seem like an ***e-mail comes from a different address than where it is actually sent from***.

Cybercriminals spoof e-mail addresses so the e-mail will ***appear to be from a trusted or familiar source***, and the e- mail's content will either contain ***links*** to ***malware*** or attempt to convince the reader to ***provide confidential information***.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

8

ACSC - Australian Cyber Security Centre

The ACSC recommends to:

Verify payment details**:** If any party to a property transaction notifies you they have updated their bank details, take extreme care to confirm changes by calling the sender's established phone number or meeting them face-to-face before transferring any funds.

Training and awareness**:** Ensure staff are trained to identify suspicious emails, including requests to change bank account details or emails linking to fake websites. The latter may be a phishing attack which could capture passwords and compromise account security.

Secure your email account**:** Knowing cybercriminals will attempt to access systems through compromised passwords, it is recommended that individuals and businesses use strong passphrases and enable or implement multi-factor authentication on email accounts to help prevent unauthorised access.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

9

Passwords

Passwords are crucially important for preventing data breaches.

There are many risks associated with 'bad' or 'weak' passwords.

Ways to ***counteract password risks*** include:

- Choose a ***different password*** for every account
- Always ***change default passwords*** that come with products during installation.
- ***Never use*** obvious passwords like "***12345***", 'Password1' or "***Admin1***
- Phrases are actually more cyber secure than the most complex password. A password is about ***8-12 characters***, often mixed heavily with alternate characters. But these passwords are common words and the substitutions are predictable. A passphrase usually has 20 characters or more.
- ***Don't ever write down your passwords*** and leave them on your workstation

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

10

Database Security

Databases contain personal data of clients, customers or employees such as their personal data, financial records, credit card numbers, etc.

Again, security can be increased by restrictions on who in the business can access the data.

Other ways to ***reduce the risks for databases*** include:

- Use database ***firewalls***.
- ***Audit*** and monitor ***database*** access ***regularly***
- Consider ***encrypting data*** at rest or data in transit. Encryption means keeping your ***data saved in a format that is unreadable and indecipherable*** to an outside hacker.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

11

Secure websites

'***Pharming***' refers to the creation of a ***fraudulent website*** that looks identical (or nearly identical) to a legitimate website.

A user is tricked into visiting the fraudulent website (***usually by clicking on a link in an e-mail***) and ***providing confidential information***, such as their login and password.

For example, a cybercriminal may target a victim using a fake website designed to look identical to the ***victim's bank's website***, tricking them into providing the login information for their bank account.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

12

BOT attacks

A ***bot*** is a ***small piece of software that automates web requests*** with various goals. Bots are used to perform tasks without human intervention, including everything from ***scanning website*** content to ***testing stolen credit card numbers*** to providing ***customer service support***. A bot can be used in both helpful and harmful ways, while "bot attack" always refers to an attacker with a fraudulent goal.

A ***bot attack*** is the use of ***automated web requests to manipulate, defraud, or disrupt a website, application,*** API (application program interfaces), or end-users.

You can locate further information about web site safety on the ACSC web site here. This information is technical in nature and provides information for web developers and security professionals, rather than the average real estate agent:

https://www.cyber.gov.au/acsc/view-all-content/publications/protecting-web-applications-and-users

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

13

Working remotely

An agency needs to ensure that individuals ***working remotely*** are working in a ***secure environment*** to ***eliminate security threats***. The risk of security breaches for remote workers can be high so some key considerations need to be covered:

1. Ensuring ***all data security practices and policies are documented*** and ***acknowledged*** by the employee and provide ***updates*** to data handling expectations during the course of employment.
2. Providing ***ample training*** on managing company data on all devices (private and company-owned) and ***proper network usage***, including ***multi-factor authentication***.
3. Providing access to key tools such as

- password management tolls
- enabling two factor authentication for all apps
- -a VPN service that can be enabled on the home router

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

14

Phishing

Phishing refers to the ***attempt*** to ***obtain personal*** or ***confidential information***, often by using a ***spoofed e-mail address***.

Phishing attempts are most commonly done through e- mail, by they ***may also*** be ***made*** through ***phone calls***, ***text*** messages, ***instant messages***, or other forms of communications.

Phishing attacks can also ***introduce malware*** by ***tricking the victim*** into ***clicking*** on a ***link*** or ***opening*** an ***attachment*** containing the malicious software.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

15

Securing Mobile Devices

Workers in the property industry are constantly using their mobile phones to carry out their job in the most time effective ways.

Cybercriminals also target mobile devices. The popularity of smartphones, including those used for business purposes, has made these devices a prime target for malware attacks.

Malware

Malware, short for "***malicious software***," can refer to any program which is ***installed on your computer without*** your ***consent*** and that ***causes harm*** to your computer. Different types of malware include:

*Spyware. 8 Adware * Ransomware * Tracking cookies * Trojan horses

* Keyloggers * Viruses * Worms

Malware programs are able to affect your computer systems in several ways, including through ***changing or hijacking primary functions, transmitting and/or deleting sensitive or private information, monitoring your online activities***, etc.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

16

Ransomware

Ransomeware is a type of *malware* and is explained as damaging software that *infects* your *computer phone* or *tablet*. There is usually a *threat* to *publish* the victim's *personal data* or *perpetually block access* to it unless a ransom is paid.

You can learn more about ransomware here:

https://www.cyber.gov.au/ransomware

You should review the following video from the Australian Cyber Security Centre which explains how ransomware works and provides 4 tips on how to protect against an attack:

https://www.youtube.com/watch?v=SV4ZZ481VAo

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

17

secure data storage

The *Office of Australian Information Commissioner* offers the below tips for compliance with maintaining security of data and records.

- barriers such as locks to *lock workstations* and *filing cabinets* when away from desks
- *security keys* and containers such as filing cabinets, safes and compactuses
- *security alarm systems* to detect unauthorised access and
- *access control* measures

These may be complimented by

- *recording file movements*, especially if files are sent to different offices
- encouraging a clean desk policy
- *storing* all *files after use* and
- a *security classification* system to identify information with special protection

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

18

Fraudulent Activity

NSW Fair Trading have *fraud prevention requirements* which are contained in the *Supervision Guidelines* and published on the Fair Trading web site: https://www.fairtrading.nsw.gov.au/__data/assets/pdf_file/0015/601233/Secretarys- Guidelines-for-the-Proper-Supervision-of-the-Business-of-a-Licensee.pdf

Section 4 of the Guidelines requires *licensees* to prepare and *maintain written procedures for agents* to correctly identify parties with whom it is planning to enter an agency agreement, such as an agreement to sell, lease or manage a property for a property owner.

As a matter of best practice, agents should *request proof of identity* when it comes to dealing with sellers or landlords, including a driver's licence or current passport, a current Medicare card or current credit card and an account statement, electoral enrolment card, gas or electricity bill or water rates. The Guidelines suggest agents should keep these identity check documents on file for inspection if required

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

19

Fraudulent Activity

Other *warning signs* of such fraud include:

- *a recent change in contact details* that are only provided with instructions to sell a property;
- transactions that involve *people or documents located overseas*, especially countries known for scams;
- a *request* for *funds* to be *deposited into a bank accou*nt *different* to the account *normally* used;
- *urgent* sales;
- *new email* addresses; and
- *comments by the seller that incentives* will be provided to the agent if the sale is quick.
- Dealing with fraud

1.Suspected Fraud - contact the NSW Police Force and immediately cease work on the sale of the property.
2.. Failure to report fraud may lead to issues with claiming on cyber security insurance.
3.You can also report via:
4.https://www.cyber.gov.au/acsc/report

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

20

Fraudulent Activities

Where there is suspected Fraud - contact the NSW Police Force and immediately cease work on the sale of the property.

Failure to report fraud may lead to issues with claiming on cyber security insurance.

You can also report via: https://www.cyber.gov.au/acsc/report

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

21

Prepare Incident response Plan

Every agency should have an incident response plan. This can include: *Educating employees* on how to recognise attacks and other forms of data breach.

How to *be prepared to handle a cyberattack*, such as *what to do immediately* if they believe an attack has occurred (e.g. who to notify and how to disconnect from the network). The plan should also *instruct employees on what not to do* (e.g. delete system files and attempt to restore the system to an earlier date).

You can read more about putting together an incident response plan here:

https://www.natlawreview.com/print/article/real-estate-industry-target-cyberattacks

and here:

https://www.securitymetrics.com/blog/6-phases-incident-response-plan

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

22

Topic 2 - Underquoting

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

23

What is Underquoting

Underquoting describes when an agent understates the estimated selling price of a property. This can cause interested buyers to waste time and money on inspecting properties, and get building reports on unaffordable properties because of vague or misleading information about the likely selling price.

Underquoting in an auction sale involves the real estate agent misleading buyers by understating property prices in a bid to increase the number of people who will compete for it at the auction, ultimately driving up the price.

Underquoting occurs when a *real estate agent either verbally advises or advertises a property for a price that is less than the estimated selling price* in the agency agreement they have with the seller. It is not considered underquoting when a property sells for a price more than what an agent estimated in the selling agency agreement.

Example: A real estate agent was fined $15,000 when caught marketing a property for $770,000, despite the sellers rejecting a $900,000 offer and setting a reserve at $950,000.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

24

The Legislation

Underquoting is illegal, both under Australian (Federal) consumer protection legislation and under the NSW agent legislation, which is the Property and Stock Agents Act 2002.

Australian Consumer Law

The Australian Consumer Law (ACL) prohibits real estate agents making representations about property prices that are *false* or *misleading* or are likely to *mislead* or *deceive*. Underquoting the likely selling price of a property for sale to a prospective buyer is false and misleading and in breach of the ACL.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

25

Property and Stock Agents Act 2002

Property and Stock Agents Act 2002

The relevant sections of the Property and Stock Agents Act 2002 (the Act) related to misrepresentation have been re-produced here, as it is very important for all agents to understand their meaning.

The crucial part of the Property and Stock Agents Act 2002 that relates to underquoting is *Division 3 Representations as to selling price*. *You are encouraged to read this Division in full here, including Section 72 Definitions through to Section 74.* You can review this here:

https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-066#pt.5-div.3

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

26

Locating information about underquoting NSW Fair Trading information for agents regarding underquoting

You should take the time to review the NSW Fair Trading document 'Underquoting guidelines for residential property' on this link.

Note that this document was produced in 2016, which was prior to NSW Fair Trading's change in name from the Property Stock and Business Agents Act to the Property and Stock Agents Act which occurred in March 2020:

https://www.fairtrading.nsw.gov.au/__data/assets/pdf_file/0010/367975/Underquoting_ guidelines_for_residential_property.pdf

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

27

Obligations of the agent

Selling price estimate must be on the agency agreement

Agents are required to include a selling price estimate on all agency agreements. The estimated selling price is your reasonable estimate of the likely selling price of the property. The estimate can be a *fixed price*, or a *range*.

When stating the estimated selling price as a range, *you must ensure the highest price in the price range does not exceed the lower price by more than 10%. Agents* should provide evidence to the seller of how they came to that estimate.

Setting an accurate estimated selling price

Your estimated selling price should only be determined after a physical inspection of the property and careful consideration of the unique factors that will affect the selling price of the property, based on your knowledge, experience and professional skills. It involves significant effort to research the latest information and an understanding of current forces at play in the market.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

28

Obligations of the agent

Look at the following in order to assist in finding appropriate selling price estimate:

- The *characteristics* and features of the property
- *Historical sales* of similar properties
- *Properties* that are available on the *current market* that are similar
- *Market demand* in the area
- *Local issues* that can influence the sales price
- Recent *valuations*
- The *circumstances* of the *seller*
- General *economic factors*
- Level of *marketing*
- Economic circumstances , interest rates and inentives
- Political circumstances such as decisions that impact on sales market e.g. negative gearing, government incentives to purchase etc.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

29

Keeping records

It is very important to always make notes in your sales file regarding sales price estimates. This way, if anyone queries the estimate, you have background information to show how you came to that figure. *Keep dates and times surrounding any conversations you have, and who is present in meetings that you have.*

NSW Fair Trading can send written notice requiring an *agent* to *provide evidence* of the *reasonableness* of any *selling price estimate made* by the agent. Note that NSW Fair Trading can also, at any point, carry out a compliance inspection of your agency and ask to view your agency's files.

Refer to Section 6 of the Supervision Guidelines for information about what must be kept in the sales file for a property:

https://www.fairtrading.nsw.gov.au/__data/assets/pdf_file/0015/601233/Secretarys- Guidelines-for-the-Proper-Supervision-of-the-Business-of-a-Licensee.pdf

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

30

Advertising Selling Price

You *cannot use* any statements such as '*offers over*' or '*offers above*'. This includes any similar words or *symbols e.g. 'plus' or '+'.*

For example: You *cannot advertise* a property as being *'$800,000 plus*' or, 'offers over $800,000' or, '$800,000 +'.

You *can* use the terms '*price guide*', '*auction guide*', '*bidding guide*' or '*price estimate*' as long as your published or stated price complies with the requirements.

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

31

Rules for updating price estimate

An agent must regularly revise their estimated selling price during the property's marketing campaign. There may be changes in the market, or buyer feedback that indicates that the agent's selling price estimate is no longer reasonable. NSW Fair Trading advise that you should review your selling price estimate on a weekly basis.

If you receive an offer on a property, or evidence potentially leads you to change your estimated selling price, you need to tell the seller as soon as practical.

If the selling price estimate needs to be *revised*, you must *give written notice to the seller and provide evidence as to why you feel your estimated selling price should be revised.* You also need to *amend* the *agency agreement* to *reflect* the revised selling price estimate.

You can do this by completing and *providing to the sel*ler (by the service of *notice requirements for the agency agreement) a 'Notice of Revision of Estimated Selling Price'*

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

32

Compliance

Breaches of the ACL for making false or misleading representations, a *corporation may be fined $10,000,000 or $500,000 for an indivi*dual.

To find out more information about the fines and penalties involved with ACL: https://www.accc.gov.au/business/business-rights-protections/fines-penalties

The maximum fine from NSW Fair Trading for underquoting is $22,000. If the matter goes to court, the agent may also lose their fees and commission from the sale, have to pay their own legal costs and potentially court costs if they are the losing party.

To find out more information about NSW Fair Trading process for prosecuting agents visit: https://www.fairtrading.nsw.gov.au/__data/assets/pdf_file/0005/922802/NSW-Fair- Trading-Prosecution-Guidelines-V7.pdf

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

33

Topic 3 – Privacy

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

34

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

35

Importance of Privacy in Aust

Privacy is an important issue for most Australians. Seventy percent consider the protection of their personal information to be a major concern in their life. The biggest privacy risks identified by Australians in 2020 are:

- identify theft and fraud (76%)
- data security and data breaches (61%)
- digital services, including social media sites (58%)
- smartphone apps (49%), and
- surveillance by foreign entities (35%) or Australian entities (26%).

Source: Australian Community Attitudes to Privacy Survey 2020 https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy- survey-2020.pdf

realfocus development partners

Mastering Influencing, Delivering Dynamic Results

36

Importance of Privacy in Aust

Three in 5 Australians (59%) have experienced problems with how their personal information was handled in the past 12 months. The majority involved unwanted *marketing communications* or having their *personal information collected* (with or *without consent*) when this was not required to deliver the service.
The behaviours Australians are most likely to consider a misuse are when:

- an organisation uses their personal information in ways that cause harm, loss or distress (84%)
- information supplied to an organisation for a specific purpose is used for another purpose (84%), and

• a personal device is listening to conversations and sharing this with other organisations without their knowledge (83%).

realfocus development partners

37

What privacy laws do you need to make sure you are complying with?

The federal privacy legislation includes:

- Privacy Act 1988
- Privacy Regulation 2013
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (the Act)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

You can view all of this legislation directly on the Federal Register of Legislation:
https://www.legislation.gov.au/

Who regulates the privacy laws?

Monitoring compliance with the privacy laws is the responsibility of the Office of the Australian Information Commissioner (OAIC) which is the independent national regulator for privacy and freedom of information:

realfocus development partners

https://www.oaic.gov.au/

38

Aust. Privacy Principles

Australian Privacy Principles

The Privacy Act includes 13 Australian Privacy Principles (APPs). You can review a Quick Reference of the Australian Privacy Principles here:
https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy- principles-quick-reference

For more detailed Guidelines on the APPs:
https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

realfocus development partners

39

Who has rights under Privacy Act

The Privacy Act regulates the way individuals' personal information is handled.

As an individual, the Privacy Act gives you greater control over the way that your personal information is handled. The Privacy Act allows you to:

know why your personal information is being collected, how it will be used and who it will be disclosed to have the option of not identifying yourself, or of using a pseudonym in certain circumstances ask for access to your personal information (including your health information) stop receiving unwanted direct marketing ask for your personal information that is incorrect to be corrected make a complaint about an organisation or agency the Privacy Act covers, if you think they've mishandled your personal information

realfocus development partners

40

Small Business & Privacy

A *small business is one with an annual turnover of $3 million or less*.

Annual turnover for the purposes of the Privacy Act includes all income from all sources.

It does not include assets held, capital gains or proceeds of capital sales.

The OAIC produce a checklist to assist a small business owner to decide whether they fall under the privacy legislation:

Do the Australian Privacy Principles apply to your agency?

The Australian Privacy Principles will apply to a real estate business if:
•It, or a related body corporate, has an annual turnover of more than $3 million; or
•It operates a residential tenancy database providing information on tenants to other people (usually subscribers to a service).

realfocus development partners

41

What is residential database ?

A real estate agent may use a residential tenancy database.

A residential tenancy database holds personal information about an individual's defaults or alleged defaults on any tenancy agreements, including damage or failure to pay rent. A real estate agent may supply this information to a residential tenancy database operator, so another real estate agent can access the information when assessing a tenancy application.

The Privacy Act covers any organisation that runs a residential tenancy database, regardless of their annual turnover.

Source: https://www.oaic.gov.au/privacy/your-privacy-rights/tenancy#WhatIsResidentialTenacyDatabase

realfocus development partners

42

Other legislation related to Privacy

Property and Stock Agents Regulation 2014
Schedule 1
1 Knowledge of Act and regulations
An agent must have a knowledge and understanding of the Act and the regulations under the Act, and such other laws relevant to the category of licence or certificate of registration held (including, laws relating to residential tenancy, fair trading, competition and consumer protection, anti-discrimination and privacy) as may be necessary to enable the agent to exercise his or her functions as agent lawfully.
7 Confidentiality
An agent must not, at any time, use or disclose any confidential information obtained while acting on behalf of a client or dealing with a customer, unless—
(a) the client or customer authorises the disclosure, or
(b) the agent is permitted or compelled by law to disclose the information.

realfocus development partners

43

Collecting information from clients and consumers

1. Collecting information from clients and consumers Open and transparent management of personal information
This relates to APP 1. This principle aims to ensure that an organisation manages personal information in open and transparent ways. They must take the necessary steps to implement these practices, procedures, and systems. Whenever you collect personal information, your agency must be transparent about why you are doing so.

Anonymity and Pseudonymity
This relates to APP 2. Any organisation collecting complaints, compliments, or any feedback about their organisation must give an individual an option for being anonymous. They can't compel anyone to disclose the identity of any individual who does not wish to.

realfocus development partners

44

THANKS for hanging out with me in your 2022-23 Compulsory CPD Training

See you again real soon…

Evelyn Olivares
0418 403 227
evelyniolivares@gmail.com

45