Pellucid Asset Management Pty Ltd

ABN: 99 684 229 534

ACN: 684 229 534

Level 1, 64-66 Foster Street, Sale 3850

Privacy

Issued | last updated	04.07.2025
Version	1.0
Responsibility	CEO | Ben Lancaster
Document management	Compliance Manager | Anthony Fleming

PART 1 - Objectives

This document

This is our Privacy policy.

Objectives

The objectives of this document are to ensure that we handle personal information consistently with the Australian Privacy Principles.

Key outcomes

The targeted key outcomes of this document are that we:

- understand privacy obligations +
- handle personal information consistently with the Australian Privacy principles.

PART 2 - What is privacy?

The word 'privacy' means different things to different people.

Types of privacy

The type of privacy covered by the Privacy Act and the Office of the Australian Information Commissioner (**OAIC**) is the protection of people's personal information.

However, this is just one aspect of privacy. Other types of privacy can include territorial privacy and physical or bodily privacy and privacy of your communications.

The OAIC generally handles privacy issues which involve a person's personal information. This can include privacy issues associated with information about your location, your health and body and your communications with others.

Our policy is directed towards the protection of people's personal information.

What is personal information?

Personal information is information that identifies you or could identify a person.

There are some obvious examples of personal information, such as name or address.

Personal information can also include medical records, bank account details, photos, videos, and even information about what a person likes, their opinions and where they work - basically, any information where they are reasonably identifiable.

Information does not have to include their name to be personal information. For example, in some cases, a date of birth and post code may be enough to identify them.

To be precise, the Privacy Act definition of personal information is:

> ".. information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

What privacy is not

The protection of your personal information privacy is different to other related concepts such as:

- confidentiality
- secrecy or
- freedom of information.

However, there can be some cross-over. If you are in doubt, speak to the Privacy Officer, Jarrah Howson.

What does the Privacy Act cover?

The Privacy Act regulates how personal information is handled. For example, it covers:

- how personal information is collected
  for example, the personal information an investor provides when they fill in one of our forms
- how it is then used and disclosed

its accuracy

- how securely it is kept
- general right to access that information.

The Act also covers more specific matters, such as:

- the use of tax file numbers
- collecting health information about an individual +
- how credit worthiness information is handled by credit reporting agencies and credit providers.

PART 3 - Australian Privacy Principles

Generally

The Australian Privacy Principles (**APPs**) are the base line privacy standards which many private sector organisations need to comply with in relation to personal information they hold.

A copy of the Australian Privacy Principles is available at http://www.privacy.gov.au.

There is also a summary of the APPs below.

More detailed information and guidance on the Office's interpretation of the APPs can be found in the Guidelines to the Australian Privacy Principles, also available at http://www.privacy.gov.au.

Not a prescriptive approach

The principles contained in the Privacy Act are not prescriptive. That is, they don't tell organisations what they must do in each situation.

Rather, they offer principles about the way in which personal information should be handled, and each agency or organisation needs to apply those principles to its own situation.

If an agency or organisation breaches the privacy principles, our Office may investigate the matter. Individuals can also make a privacy complaint to us about an agency or organisation if they think their information has been mishandled. See Complaints.

APP summary

There are 13 APP that regulate how private sector organisations manage personal information.

They cover the collection, use and disclosure, and secure management of personal information.

They also allow individuals to access that information and have it corrected if it is wrong.

Part 1

Consideration of personal information privacy

Australian Privacy Principle 1

Open and transparent management of personal information

The object of this principle is to ensure that we manage personal information in an open and transparent way, enabling us to comply with the Australian Privacy Principles and deal with inquiries or complaints from individuals about our compliance with the Australian Privacy Principles on our website.

Australian Privacy Principle 2

Anonymity and pseudonymity

When we collect personal information it is because we are required under Australian law or a court/tribunal order to deal with individuals who identify themselves. It follows that when dealing with us, individuals do not have the option of not identifying themselves.

Part 2

Collection of personal information

Australian Privacy Principle 3

Collection of solicited personal information

The object of this principle is to ensure we only collect information reasonably necessary for one or more of our functions. We must not collect sensitive information without the individual's consent, and collection of personal information must occur only by lawful and fair means.

Australian Privacy Principle 4

Dealing with unsolicited personal information

If we receive unsolicited personal information, we must determine whether it could lawfully have been obtained under APP 3. If not, we must, as soon as is practicable, destroy the information or ensure that it is de-identified.

Australian Privacy Principle 5

Notification of the collection of personal information

This principle ensures that individuals are aware of the collection of personal information, at or before the time of collection. They must be alerted as to the purposes for which we require the information, the consequences if the information is not collected, others we may disclose this information to, and the guidelines in our policy regarding access and complaints.

Part 3

Dealing with personal information

Australian Privacy Principle 6

Use or disclosure of personal information

We must not disclose or use any personal information with consent from the individual, or under a reasonable expectation that the information will be used for a secondary purpose. In each case, we must take reasonable steps to ensure the information is de-identified.

Australian Privacy Principle 7

Direct marketing

Personal information must not be used for the purpose of marketing, except where there is a reasonable expectation for it to be used as such, or if the individual has given us permission.

Australian Privacy Principle 8

Cross, border disclosure of personal information

The object of this principle is to ensure that before we disclose any personal information to an overseas recipient, we must take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information.

Australian Privacy Principle 9

Adoption, use or disclosure of government related identifiers

We must not adopt a government related identifier of an individual as our own identifier the individual, unless authorised.

Part 4

Integrity of personal information

Australian Privacy Principle 10

Quality of personal information

We must take reasonable steps to ensure that the personal information we collect and use or disclose, is accurate, up to date, complete and relevant.

Australian Privacy Principle 11

Security of personal information

This principle ensures we take reasonable and appropriate steps to protect any personal information from misuse, interference, loss, or unidentified access.

It also ensures that we take reasonable steps to destroy or de-identify any information no longer needed but we need not do so where:

- the information is contained in a Commonwealth record, or
- we are required by or under an Australian law, or a court/tribunal order, to retain the information.

Part 5

Access to, and correction of, personal information

Australian Privacy Principle 12

Access to personal information

If we hold personal information about an individual we must, upon request, give the individual access to the information. Exceptions to access will occur if we reasonably believe the information will be used unlawfully, or there is a conflict of interest.

Australian Privacy Principle 13

Correction of personal information

If we are confident that personal information we hold is inaccurate, out of date, incomplete, irrelevant or misleading, we must take necessary and reasonable steps to correct that information.

PART 4 - Scope of the regime

The Privacy Act

The Privacy Act regulates 'information privacy'. It covers a number of different activities and sectors.

Who has rights under the Privacy Act?

Individuals have rights under the Privacy Act, which give them greater control over the way their personal information is handled.

As an individual, the Act allows you to:

- know why your personal information is being collected and how it will be used
- ask for access to your records (including your health information)
- stop receiving unwanted direct marketing material
- correct inaccurate information about you +
- ensure your information is only used for purposes you have been told about.

Who has responsibilities under the Privacy Act?

Australian and ACT government agencies and certain private sector organisations have responsibilities under the Privacy Act.

We have elected to have a policy consistent with the APPs.

PART 5 - Our privacy policy

Background

We respect rights to privacy concerning personal information we hold about them. This Part 5 is our privacy policy.

We may hold personal information about people, principally because they are a client or shareholder or they give us information, for example through our web site.

We aim to manage personal information in an open and transparent way.

Our goal is to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to our functions and activities that will ensure that we comply with the Australian Privacy Principles, and as will enable us to deal with inquiries or complaints from individuals about our compliance.

This document

This document outlines how we manage personal information which we hold.

Broadly, we collect, hold, use and disclose your personal information for purposes related to the provision of services to clients and shareholders and others.

Details follow.

Things change

It's very important that you keep us up to date with your details. If our details about you are wrong, we will correct them free of charge if you let us know.

Investors must in a timely way give all information that we reasonably request to perform our functions.

Why is personal information collected?

Broadly, we use personal information to provide financial services and related purposes, for example to:

- make the use of our web site easier
- contact investors regarding services from us or our affiliates
  investors can opt out of these communications
- comply with legal obligations and
- conduct research.

We also use personal information for other reasons such as:

- monitoring, evaluating and improving products and services
- statistical, actuarial, prudential or research and
- to provide you information about other services and products.

If you do not provide us with contact details and other information we ask for, we (or others) may not be able to have or keep you as a client or shareholder or provide services to you.

How we collect

There are several ways we collect personal and other information but we aim to ensure they are lawful and fair means:

Usually we end up holding personal information about you when:

- Equity Trustees or the Administrator gives it to us,
- you give it to us,
- someone you have given it to, like your financial adviser, gives it to us,
- someone you have given permission to share it, like an advertiser, gives it to us, or
- you respond to our or our affiliates marketing or other communications.

Our clients and shareholders as well as those who help us and them provide products and services to you can also collect personal information and pass it on to us.

We do not give personal financial advice and are generally not aware of our client's objectives, financial situation or needs.

In agreeing for us to provide services to you, you consent to the collection by us of information from someone other than you whom we have no reason to doubt properly represents you
for example, someone investing jointly with you, your relative, your trustee or administrator, your financial, legal or other adviser, if a trustee, your beneficiary, your partners, your investors, someone authorised to operate your account or your broker.

Unsolicited personal information which we could not have collected under the Australian Privacy Principles is destroyed or de-identified if it is lawful and reasonable to do so.

What is collected and held

We only collect personal information which we consider reasonably necessary for one or more of our functions or activities.

Personal information collected can include the following:

- name, gender and date of birth
- contact details
- Emails
- use details for our website
- any other information that we consider necessary or desirable.
- information contemplated by laws and regulator, settlement system or exchange policies and requests.

In operating the Fund, the Responsible Entity or those who work for it such as the Fund administrator may collect additional personal information, which may include the following and which is governed under their privacy policy is available on their websites:

- TFNs and ABNs
- details of your investors and beneficiaries
- details of the source and use of money you invest

Because of the requirements of law, it may be impracticable for us to deal with individuals who have not identified themselves or who have used a pseudonym.

When we use and disclose

We will seek to ensure that your personal information is not used or disclosed for any purpose other than:

- the primary purpose for which it was collected or a purpose that is related to the primary purpose for which it was collected or a related secondary purpose,
- where you have consented to the use or disclosure, or
- in other circumstances where the Australian Privacy Principles authorise the use or disclosure such as when it is required by or authorised under law.

We will not disclose personal information we hold about you unless:

- this document allows,
- you otherwise agree,
- we consider someone needs the information. typically because they are a regulator, settlement system or exchange or your adviser or to assist us - for example the Fund administrator of one of our investment products you have invested in, or
- laws or regulator, settlement system or exchange policy requires, or a regulator, settlement system or exchange requests and
- to administer your investment.

Those we disclose personal information to include:

- our clients and shareholders and those that assist them
- regulators, settlement system or exchanges
  such as AUSTRAC, the ASIC, the OAIC and APRA,
- your financial or other adviser,
- those we have no reason to doubt are acting on your behalf,
- companies with our group, and
- those who help us provide products and services to you
  for example, distributors, superannuation fund trustees, insurance brokers, insurance companies, fund managers, custodian, fund administrators, mailing houses and auditors.

We may provide website usage information about visitors of our website to third-party ad servers for the purpose of advertising.

In the case of joint accounts, we allow each individual access to account balances and transaction details, but not to the personal details of the other individual.

How we hold

We keep physical records on premises or in commercial storage.

Electronic records are kept on local servers, with back-ups off site.

No personal data is stored on our web site.

Some of the measures that we have adopted are having facilities for the secure storage of personal information, having secure offices and access controls for our computer systems.

We will also take reasonable steps to destroy or permanently de-identify personal information that we no longer need for any purpose for which may be used or disclosed under the Australian Privacy Principles.

Retaining, deleting and depersonalising records

Context

As a general rule information gathered from applicants in the Fund is held not by us, but rather by the Responsible Entity and its registry provider. This will include all the information gathered by application forms and online application processes. The Responsible Entity may share personal information with us, but again this will be relatively limited.

Deleting and depersonalising

Consistent with the privacy principles, we take reasonable steps to destroy or permanently de-identify personal information if we no longer need it for any purpose for which we may use or disclose the information.

However the privacy principles do not require us to take these steps where:

- the information is contained in a Commonwealth record, which will include information available from or under or relating to:
    - bankruptcy, administration and insolvency
    - births, deaths and marriages
      including names and former names, marital status, date and place of birth
    - business and company records
      eg ASIC, NSW Department Of Fair Trade, and including residential addresses, principal places of business and registered offices as well as ABNs
    - Occupational records
      eg financial advisers, health practitioners, builders and tradespeople, conveyances, company directors, real estate agents, or
- we are required by or under an Australian law, or a court/tribunal order, to retain the information
  see 'Retaining records' below

Information not generally available on public registers includes information we may hold:

- email address and potentially contact phone number

as well as information we generally do not hold (but the Responsible Entity may) such as:

- bank account details
- employment information
- trust beneficiaries
- the source and use of money invested
- sexual preference
- Drivers licence and passport numbers
- Medicare number
- motor vehicle ownership
- credit score.

As a general rule, we cease marketing to a person using their personal information six years after the latest of:

- if we have had no engagement from them, the end of the calendar year that is 6 years after the year we commenced marketing to them, or
- if we have had engagement from them, the end of the calendar year that is 6 years after the year we last engaged them

Retaining records

In the absence of specific requirements, we generally take our lead as to the time for retaining records from a relevant limitation. Records may include personal information.

A limitation period refers to the maximum period of time that can pass from the time a cause of action occurs until the start of court proceedings relating to that cause of action. The factors that determine limitation periods include the nature of the matter and the governing legislation.

Limitation periods, and specific obligations to retain records, vary from jurisdiction to jurisdiction, and depend on the particular reason for which records were created or the basis from which any claims are made.

As a general rule we retain records on the following basis:

- Contractual matters: 6 years
- deeds: 12 years
  for example, trust dates, confidentiality deeds, days of settlement and deeds of indemnity and guarantee
- negligence: 6 years
- Misleading and deceptive conduct under the ASIC Act: 6 years
- taxation matters: 5 years.

We note that we are not a trustee however:

- claims for specific performance, injunctions and general equitable relief in relation to trusts have no specific limitation period,
- claims of breach of trust generally have a limitation period of six years
  unless otherwise fixed by relevant law, and
- claims by trustees and beneficiaries for fraud, fraudulent breach of trust, conversion and respective trust property generally have a limitation period of 12 years
  unless otherwise fixed by relevant law.

What about security?

We are committed to ensuring that personal information is kept secure. We take reasonable steps to ensure that the personal information that we hold is protected from misuse and loss and from unauthorised access, modification and disclosure.

We have a number of physical access and technology policies and procedures in place designed to provide a robust security environment.

No personal data is stored on our web site.

We will communicate with investors by email from time to time. On our website, investors are advised that email can be insecure.

We may store personal information in the cloud. This involves some risks, and on our website, investors are advised that we are not responsible for those providers or data use or loss by them.

A note about the internet

The internet is not a secure environment and we cannot guarantee the security of information we exchange electronically. This is the nature of the Internet.

It is possible however that your personal information will be moved by those who help us provide products and services to you to a place where Australian laws do not apply, and different standards may apply there.

Records may be stored in the cloud, in Australia or overseas (as is the nature of storage such as this), by us as well as those who help us provide products and services to you. We will tell you what cloud providers are used if you ask, and direct you to their information policies on personal information.

It is not practicable to tell you the countries where that information is likely to be located.

The internet does not however always result in a secure information environment and although we take steps we consider reasonable to protect your information, we cannot absolutely guarantee its security.

We may use “cookies” to obtain information with regards to web site activity (such as the type of browser used, the number of pages viewed, time of the site and navigation patterns), and to help you use this site when you visit again. This information on its own does not identify an individual but it does provide us with statistics that can help us with the design of the web site. You can configure your browser to accept or reject cookies. If you reject all cookies you may not be able to use some or all of our website.

Offshore rules

We are an Australian business and engaging with us is on the terms of Australian law.

We do not conduct a business anywhere else except in Australia, but the Internet has no boundaries - our website is visible from around the world - and as a general rule we do not inquire as to the physical location of people who interact with us.

We may from time to time seek to comply with laws of other jurisdictions as far as practicable where we believe that failing to do so may have a material adverse impact on our business but as a general rule there is no obligation for us to do so.

Sensitive information

Sensitive information is a sub-set of personal information, and is given a higher level of protection under the Australian Privacy Principles.

It is information or an opinion about:

- racial or ethnic origin,
- political opinions,
- membership of a political association,
- religious beliefs or affiliations,
- philosophical beliefs,
- membership of a professional or trade association,
- membership of a trade union,
- sexual preferences or practices,
- criminal record, or
- biometric and health information.

It would be very rare that we collect sensitive information.

We only ever collect sensitive information about an individual if:

- the individual consents to the collection and the information is reasonably necessary for our functions or activities,
- if required or authorised by or under an Australian law or a court/tribunal order,
- there is a serious threat to their life, health or safety,
- we suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being or may be engaged in, or
- the collection is reasonably necessary to assist to locate a missing person.

Links to other web sites

Our website may contain links to other web sites for your convenience. We are not responsible for the information handling and privacy policies and practices of other linked web sites.

Telephone services

We may monitor or record telephone calls for training, record or security purposes. If we do so, we will tell you at the time.

Access to personal information

In most circumstances, you have the right to access any personal information we collect and hold about you, and to have it corrected if it is wrong.

This is subject to exceptions allowed by law such as where giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety or where providing you with access would have an unreasonable impact upon the privacy of others.

If we deny your request or access we will provide you with the reasons for this decision.

To request access please contact us and we will respond within a reasonable period after the request is made.

Correcting personal information

We endeavour to take reasonable steps to ensure that the personal information that we collect, use or disclose is accurate, up to date, complete, relevant and not misleading.

If you believe that any of the personal information that we hold about you is not accurate, complete, up-to-date or is misleading please contact us.

If we agree that the personal information requires correcting we will take reasonable steps to do so.

If we do not correct your personal information we will provide you with the reasons for not doing so. If you request that we associate with the information a statement claiming that the information is not accurate, complete and up-to-date we will take reasonable steps to comply with this request.

Reporting breaches

We have administrative processes in place which are designed to identify breaches of privacy law and ensure that we notify to regulators those breaches which are required to be notified. See our **Policy | Breaches and whistle blowing.**

Acting reasonably

We may take and may act (or not act as relevant) on any advice, information and documents which we have no reason to doubt as to authenticity, accuracy or genuineness.

About this document

This Part of this document is the privacy policy for Pellucid. It is current as at the date on the front cover. If you would like a copy, contact us and we will email or post it to you free.

We may make changes to information handling and privacy policies and practices and this Privacy Policy Statement. We will publish important changes on our web site and if necessary update this Privacy Policy.

Changes

We may make changes to information handling and privacy policies and practices and this privacy policy.

We will publish important changes on our web site and if necessary update this document.

Privacy Officer

We have appointed [privacy officer full name]as the Privacy Officer. Their role is to:

- with the Compliance Manager | Anthony Fleming keep this document up to date,
- ensure our systems are consistent with this document,
- recommend changes as needed,
- manage enquiries and complaints, and
- ensure it is understood by our officers.

Questions and complaints

Be mindful that if you are an investor in what about funds, then as a general rule you should contact the Responsible Entity of those funds if you have a complaint which concerns the Fund. For the most part, they rather than us will hold the vast majority of personal information about you, because you are an investor in a fund that they operate. You can find out how to contact them about your privacy concerns or questions from their websites or from each Fund's PDS.

If you're unsure, or if you do have a complaint about privacy which concerns us, then please contact us. You can obtain further information about the way in which we manage personal information that we hold, or you can raise any privacy issues with us (including any concerns you may have about breaches of the Australian Privacy Principles), by contacting us in writing:

The Privacy Officer
Pellucid Asset Management Pty Ltd
Level 1, 64-66 Foster Street, Sale 3850
Email: [privacy email]

Attachment 1

What are permitted general situations?

The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' exists.

This exception applies in relation to the collection of sensitive information (APP 3), the use or disclosure of personal information (APPs 6 and 8) and the use or disclosure of a government related identifier (APP 9).

It is nevertheless open to an APP entity to comply with the APP requirements even though an exception applies.

Lessening or preventing a serious threat to life, health or safety

This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and
- the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A, Item 1).

Unreasonable or impracticable to obtain consent

Consent is defined as 'express consent or implied consent' (s 6(1)) and is discussed in Chapter B (Key concepts). The main criteria for establishing consent are:

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

An APP entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain an individual's consent. Relevant considerations may include:

- the nature of, and potential consequences associated with, the serious threat. For example, the urgency of a situation and level of threatened harm may require collection, use or disclosure before it is possible to seek consent
- the possible adverse consequences for an individual if their consent is not obtained before the collection, use or disclosure. It may be more difficult for an entity to establish that it was unreasonable or impracticable to obtain the individual's consent as the risk of adversity increases
- the source of the threat. For example, it may be unreasonable to seek consent from the individual posing the threat where that individual could reasonably be anticipated to withhold consent, or where the act of seeking that individual's consent could increase the threat
- the ability to contact the individual to obtain consent. For example, it may be impracticable to obtain consent if the individual's location is unknown after reasonable enquiries have been made, or if they cannot be contacted for another reason

- the capacity of the individual to give consent. For example, it may be unreasonable or impracticable to obtain consent where an individual is incapable of communicating consent because of their physical or psychological state or their age (capacity is discussed as part of 'consent' in Chapter B (Key concepts))
- the number of individuals whose personal information is to be collected, used or disclosed. For example, it may be impracticable to obtain consent from a very large number of individuals (though see below as to the relevance of inconvenience, time and costs)
- the inconvenience, time and cost involved in obtaining consent. However, an entity is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Reasonably believes collection, use or disclosure is necessary

Where it is unreasonable or impracticable to obtain consent, an APP entity must reasonably believe the collection, use or disclosure is necessary to lessen or prevent a serious threat. The terms 'reasonably believes' and 'necessary' are discussed in Chapter B (Key concepts).

In summary, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of an APP entity to be able to justify its reasonable belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient.

Lessen or prevent a serious threat

This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. A 'serious' threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease. This allows an APP entity to take preventative action to stop a serious threat from escalating before it materialises.

The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person's physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation.

The threat may be to an individual the APP entity is dealing with or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly.

C.12 A 'serious threat to public health or safety' relates to broader safety concerns affecting a number of people. Examples include:

- the potential spread of a communicable disease
- harm, or threatened harm, to a group of people due to a terrorist incident
- harm caused by an environmental disaster.

C.13 If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure, before relying on this permitted general situation.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

C.14 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being, or may be engaged in, and
- reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A, Item 2).

C.15 This permitted general situation is intended to apply to an APP entity's internal investigations about activities within or related to the entity. It applies when the entity has reason to suspect unlawful activity, as well as misconduct of a serious nature that does not necessarily amount to unlawful activity.

C.16 'Unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass. The unlawful activity must relate to the APP entity's functions or activities. For example, harassment or discrimination within an entity would be an unlawful activity.

C.17 'Misconduct' is defined in s 6(1) to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. 'Serious' misconduct does not cover minor breaches and transgressions. The serious misconduct must relate to the APP entity's functions or activities. For example, a serious breach by a staff member of the Australian Public Service Code of Conduct, or fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities.

C.18 An APP entity must have 'reason to suspect' that unlawful activity or serious misconduct is being, or may be engaged in. Though only a reasonable suspicion is required, it is the responsibility of the entity to be able to justify the suspicion.

C.19 An APP entity must 'reasonably believe' that the collection, use or disclosure of personal information is 'necessary' for the entity to take 'appropriate action'. 'Reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts). In summary, there must be a reasonable basis for the belief that the collection, use or disclosure is necessary, and not merely a genuine or subjective belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of an entity to be able to justify its reasonable belief.

C.20 Whether action is 'appropriate' will depend on the nature of the suspected unlawful activity or misconduct and the nature of the action that the APP entity proposes to take. Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority. For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply.

Locating a person reported as missing

C.21 This permitted general situation applies when an APP entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing. The collection, use or disclosure must comply with the rules made by the Information Commissioner under s 16A(2) (s 16A, Item 3).

C.22 The terms 'reasonably believes' and 'reasonably necessary' are discussed further in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief that the collection, use or

disclosure is reasonably necessary, and not merely a genuine or subjective belief. 'Reasonably necessary' has regard to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an entity to be able to justify that the entity reasonably believes that the collection, use or disclosure is reasonably necessary.

C.23 The rules made by the Commissioner under s 16A(2) are a legislative instrument that are available on the Comlaw website.

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

C.24 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A, Item 4).

C.25 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.26 This permitted general situation applies to the collection, use or disclosure of personal information in relation to existing or anticipated legal proceedings in a court or tribunal. Where legal proceedings have not yet commenced, this situation will usually only apply to a collection, use or disclosure involving a real possibility of legal proceedings, for example where professional legal advice is sought about commencing legal proceedings. By contrast, this permitted general situation does not compel an APP entity to disclose personal information in response to a request from a third party, and it may be difficult for an entity to be satisfied that it is reasonably necessary to do so solely on the basis that a third party has requested the information in connection with existing or anticipated legal proceedings.

C.27 An APP should not rely on this permitted general situation to disclose personal information if doing so would be contrary to an Australian law (for example, a statutory secrecy provision) or a legal order or principle (for example, if disclosure would be a breach of legal professional privilege).

Reasonably necessary for a confidential alternative dispute resolution process

C.28 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the purposes of a confidential alternative dispute resolution process (s 16A, Item 5).

C.29 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.30 The phrase 'alternative dispute resolution process' (or ADR) is not defined in the Privacy Act. ADR covers processes, other than judicial determinations, in which an impartial person assists those in a dispute to resolve the issues between them. That person may, but is not required to, have any particular form of accreditation.

Examples of ADR processes include mediation, conciliation, facilitation, expert assessment, determination, or neutral evaluation.

C.31 For the exception to apply, the parties to the dispute and the ADR provider must be bound by confidentiality obligations such that any personal information collected, used or disclosed for the purpose of that ADR process will not be used or disclosed for any purpose outside the ADR process, including use or disclosure in subsequent proceedings. The confidentiality obligations may be imposed through contractual agreements or legislative provisions.

C.32 This permitted general situation extends to a disclosure of personal information by an APP entity to an ADR provider, a collection, use or disclosure by an entity for the purpose of participating in the ADR, and the collection, use or disclosure by an entity in relation to a complaint of professional misconduct against an ADR practitioner.

Necessary for a diplomatic or consular function or activity

C.33 This permitted general situation applies when an agency reasonably believes that the collection, use or disclosure of personal information is necessary for the agency's diplomatic or consular functions or activities (s 16A, Item 6). This permitted general situation applies only to agencies, and not to organisations. The terms 'reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts).

C.34 The terms 'diplomatic' and 'consular' are not defined in the Privacy Act. An agency can rely on this permitted general situation only if it has diplomatic or consular functions or powers, conferred either by legislation or an executive instrument (such as the Administrative Arrangements Order). The following are given as examples of when this permitted general situation might apply:

- Diplomatic functions or activities: where an agency collects, uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.
- Consular functions or activities: where an agency collects, uses or discloses personal information to:
    - assist Australian citizens who are in distress overseas, including where an Australian individual is detained or is the victim of crime, or where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas
    - provide information to the next of kin of an Australian individual who is overseas where, for example, the individual is seriously injured or is suffering serious physical or mental illness, and the agency considers that there are likely to be significant, serious or undesirable consequences for the individual or their next of kin if it does not disclose the personal information.