PRIVACY POLICY

Policy

What Types of Information are Covered by Privacy Laws?

Privacy is all about how we handle the personal and sensitive information we collect from you.

The way we do this is set out in the section ‘How do we handle Personal Information’.

We have a legal obligation, under the Privacy Act, to handle the personal information (including sensitive information) we collect about individuals in accordance with the 13 Australian Privacy Principles (APPs), where that information is included in a record.

What is Personal Information?

Personal Information is information, or an opinion, about an identified individual, or an individual who is reasonably identifiable:

- whether the information, or opinion, is true or not; and
- whether the information, or opinion, is recorded in a material form or not.

The Privacy Act only applies to personal information that is captured in a record.

Personal Information

- will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances
- includes information such as a person’s name, address, financial information, marital status, or billing details
- includes an opinion, for example, survey results
- can be stored using any medium e.g. in a database, email, paper, or on disk
- includes sensitive information about individuals.

Personal Information does not include information that has been de-identified.

The types of personal information we collect are noted below.

What is Sensitive Information?

- health
- ethnicity
- religion
- political opinion

- sexual preferences
- criminal record
- genetics
- biometric identification
- membership of professional association

Note: Sensitive information is generally afforded a higher level of privacy protection.

The types of sensitive information we collect are noted in this Policy.

The Privacy Act also includes health information, a subset of sensitive information, however IML does not collect such information.

What is Confidential Information?

Confidential information is not a term that is defined within the Privacy Act.

In simple terms, personal information does not include confidential information relating to a business, unless the confidential information is about individuals and falls under the definition of Personal Information, Sensitive Information, or Health Information.

What is a Record?

It is important to note that the Privacy Act only regulates personal information that is contained in a "record". "Record" is a defined term in the Privacy Act and includes a document, a database (however kept), a photograph or other pictorial representation of a person. It is interpreted widely and will include anything stored on an electronic device such as a mobile phone.

Whose Information is Protected by the Privacy Act

The Privacy Act requires us to protect all personal information (including sensitive information and health information) about any individuals who deal with us.

Who Do We Collect Personal Information From?

At Investors Mutual Limited we collect personal information from customers, including potential customers, who we provide, or may provide, a financial service

We are also likely to collect personal information from others including:

- contractors
- board / committee Members
- job applicants
- staff members

Identifying an Individual

The term ‘individual’ is defined in the Privacy Act as any natural living person including:

- people who are sole traders and people trading in partnerships
- people who represent companies and other organisations, but do not include the company or organisation itself
- job applicants up to the point they become our employees. As noted below, the exemption for employees only relates to employee records used directly in the context of the employment relationship.

When is an Individual ‘Reasonably Identifiable’?

Whether an individual is ‘reasonably identifiable’ from particular information will depend on a number of considerations including:

- the nature and extent of the information
- the circumstances of its receipt by us

Whether it is possible for us to identify the individual using available resources, taking into account the cost, difficulty, practicality, and likelihood of us doing so.

Our Privacy Officer

The Head of Risk & Compliance is our Privacy Officer.

Our Privacy Officer can be contacted at:

- Level 24, 25 Bligh Street Sydney 2000
- 02 8224 0508

Our Privacy Officer is Responsible for:

- promoting a culture where the personal information of individuals is protected in accordance with our obligations under the Privacy Act
- integrating privacy obligations into existing practices and procedures and policy documents
- providing or organising ongoing training support for managers to ensure that all relevant persons receive privacy training
- managing privacy queries and complaints
- liaising with regulators (where necessary)
- monitoring privacy compliance performance
- analysing performance to identify the need for corrective action
- ensuring privacy issues are factored into contracts with external suppliers
- ensuring our privacy program and privacy policy is reviewed on a regular basis

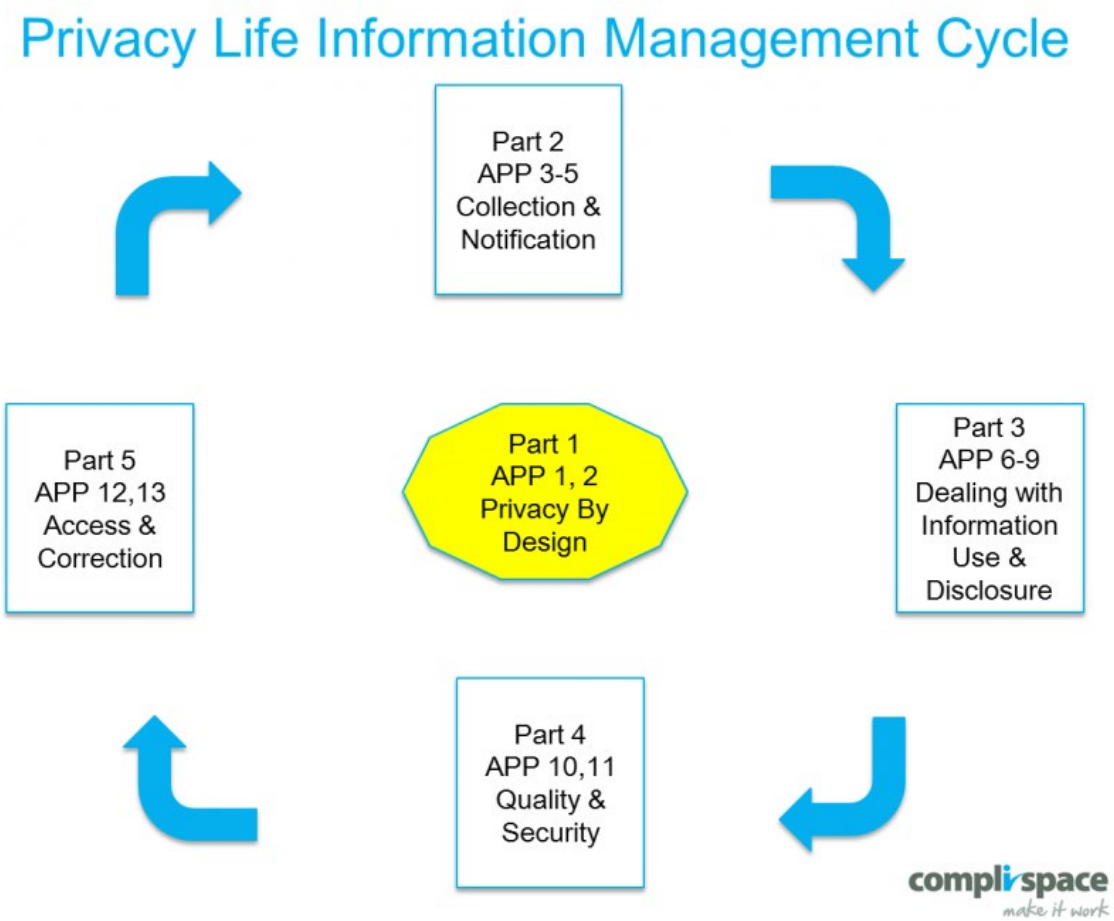
An Overview of the Australian Privacy Principles (APPs)

The 13 Privacy Principles set out how we handle the personal information we collect and use about individuals.

The Australian Privacy Principles (APPs) can be categorised into five parts as follows:

Part 1- Privacy by Design APPs 1 & 2
Part 2- Collection and Notification APPs 3, 4 & 5
Part 3- Dealing with Information Use & Disclosure APPs 6, 7, 8, & 9
Part 4- Quality and Security of Information APPs 10 & 11
Part 5- Access to and Correction of Information APPs 12 & 13

These five parts follow a Privacy Information Management Life Cycle as illustrated in the following diagram:



How We Handle Personal Information

Principle 1: Open and Transparent Management of Personal Information

The Legal Requirement:

Investors Mutual Limited must establish and effectively implement practices, procedures, and systems that ensure:

- we comply with each of the 13 APPs
- we can deal with inquiries or complaints from individuals about our compliance

The objective of this principle is to ensure that we manage personal information in an open and transparent way.

How We Comply with This Obligation

Investors Mutual Limited is committed to managing personal information in an open and transparent way, and to this end we have adopted the “privacy by design” approach required under APP 1, which allows us to effectively manage personal information in accordance with the 13 APPs.

Our Internal Practices, Procedures, and Systems

Internal practices, procedures, and systems that we have implemented include:

- the establishment of this Privacy Program which sets out how we comply with each of the 13 APPs set out in the Privacy Acts
- the publication of our Privacy Policy through which we disclose how we manage personal information on a day-to-day basis
- the development of privacy consents that give the individual the opportunity to choose which collections, uses, and disclosures they consent to. Note: We do not use the practice of “bundled consents” as they have the potential to undermine the voluntary nature of consent
- the establishment of a Risk Management Program that substantially meets the guidelines as set out in the International Risk Management Standard AS/NZ ISO 31000: 2009, through which we manage privacy related risks
- the establishment of a Compliance Program which substantially meets the guidelines as set out in the Compliance Management Systems 19600:2015. Our Compliance Program is designed to ensure legal and regulatory, organisational and contractual compliance including compliance with APPs
- the establishment of an AML/CTF Program which meets the requirements of the AML/CTF Act and Rules. Our AML/CTF Program includes procedures to deal with the information we are required to collect and verify under the AML/CTF Act and Rules
- the establishment of a Complaints Handling Program that substantially meets the guidelines as set out in the Australian New Zealand ISO AS 1SO 10002: 2014, through which we manage privacy related complaints

- the development of Privacy Training to ensure key aspects of our Privacy program are effectively communicated to staff
- the development of associated policies and procedures designed to ensure compliance with the privacy laws which are integrated into our day-to-day operations
- regular management and Board reporting with respect to Risk and Compliance issues, including privacy, where applicable
- regular review of our Privacy Program and our Privacy Policy (as well as associated policies) to ensure that they remain relevant and continue to ensure our ongoing compliance with privacy laws

Our Privacy Policy

Investors Mutual Limited has developed a Privacy Policy that sets out how we manage personal information. A copy of Privacy Policy is available on our public website on www.iml.com.au or alternatively, to request a copy to be sent by email or post, please email the IML Privacy Officer at privacy@iml.com.au. Once we receive a request, our Privacy Officer will review the request and provide a copy of the Policy in a format that the person requested.

Our Privacy Policy Outlines

- who we collect information from
- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use and/or disclose personal information
- how an individual can access their personal information and seek a correction of information
- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients and if so, the countries in which those recipients are based

Our Privacy Policy is available free of charge. A copy of Privacy Policy is available on our public website on www.iml.com.au/privacy-policy or alternatively, to request a copy to be sent by email or post, please email the IML Privacy Officer at privacy@iml.com.au. Once we receive a request, our Privacy Officer will review the request and provide a copy of the Policy in a format that the person requested.

Principle 2: Anonymity and Pseudonymity

The Legal Requirement:

We must guide individuals dealing with Investors Mutual Limited the option of not identifying themselves or the option of using a pseudonym unless:

- we are required by law to deal with individuals who have identified themselves (such as the customer identification requirements under the AML/CTF Act)
- it is impractical for us to deal with an individual who does not identify themselves or uses a pseudonym

How We Comply with This Obligation

In rare cases, individuals dealing with Investors Mutual Limited may have the option of doing so anonymously or by using a pseudonym.

The effect of an individual opting to deal with us in this way is that the individual's personal information or identifiers cannot be collected, thereby allowing the individual to exercise greater control over their personal information.

Investors Mutual Limited is required to make all individuals aware of this option and we do so through our Privacy Policy.

In circumstances where it is impractical for Investors Mutual Limited to deal with individuals who have not identified themselves (e.g. a complaint may not be able to be investigated and resolved without identifying the complainant) or where we are required by law or court order to deal with identified individuals only, then individuals will not have the option of retaining anonymity or using a pseudonym.

Specifically, where we are required to collect an individual's personal information under the AML/CTF Act and Rules, then the individual will not have the option of retaining anonymity or the use of a pseudonym.

Principle 3: Collection of Solicited Personal Information

The APPs differentiate between "solicited information" and "unsolicited information".

Solicited Information is information we have asked an individual to provide to us. Solicited Information is dealt with under APP 3.

Unsolicited Information is information that has been provided to us, by an individual, without us requesting the information. Unsolicited information is dealt with under APP 4.

The Legal Requirement:

Investors Mutual Limited must not collect solicited personal information (including sensitive information) unless the information is reasonably necessary for one or more of our functions or activities.

Generally, we must not collect sensitive information unless the individual has consented, it is required by law, or if it is impractical to obtain the individual's consent, the information is necessary to prevent or lessen a serious threat to the life or health of an individual.

We must only collect personal information by lawful and fair means and not in a way that can be interpreted as unreasonably intrusive.

Unless we have obtained an individual's consent, we must only collect their personal information directly from them, unless it is unreasonable or impractical to do so.

How We Comply with This Obligation

Personal Information we Actively Collect

Investors Mutual Limited only actively collects personal information (including sensitive information) that is reasonably necessary for one or more of our functions or activities.

If the personal information is sensitive information (including health information), then we obtain the individual's consent (which may be implied) to the collection, unless:

- the collection of the sensitive information is required by law
- it is unreasonable or impractical to obtain the individual's consent and the collection is necessary to prevent or lessen a serious threat to life or health of an individual
- other specific circumstances exist for sensitive information which is health information.

Refer to the Privacy Commissioner's APP Guidelines for **Permitted General Situations.**

For details on the types of personal, sensitive, and health information we collect refer to **What Types of Information are Covered by Privacy Laws.**

How We Collect Personal Information

We may collect personal information any time we deal with an individual, (including when meeting our initial and ongoing customer due diligence obligations under the AML/CTF Act).

We are committed to ensuring that collection only occurs by fair and lawful means including:

- by phone
- by email
- by mail
- using an application form
- in face-to-face meetings with an individual

We must be careful when collecting sensitive information, that we do not do so in the presence of others, and that we do not advise an individual that it is compulsory to provide information when it is not. Such actions may be considered unfair or unreasonably intrusive.

Collection Through Surveillance

Investors Mutual Limited has developed the following policies that deal with the collection of personal information through surveillance:

IT Support & Usage Policy

Collection of Information Directly from the Individual

The Privacy Laws require that personal information must be collected directly from an individual unless it is unreasonable or impractical for us to do so.

Whether it is unreasonable or impractical to collect personal information directly from any individual will depend on a range of considerations including:

- the difficulty of collecting the information from the individual
- whether the individual would reasonably expect the information to be collected from them or another source
- the sensitivity of the information
- whether direct collection would jeopardise the integrity of the information or the purpose of collecting it
- whether the cost of collecting the information directly would be excessive

Principle 4: Dealing with Unsolicited Personal Information

Investors Mutual Limited may also receive personal information about an individual in circumstances where we have taken no active step to collect the information. This is known as unsolicited personal information.

Examples of unsolicited personal information we may collect include:

- additional information collected in our customer onboarding procedures
- a promotional flyer/leaflet promoting an individual’s business containing an email address or a mobile phone number
- personal information that is provided to us that is additional to the information solicited by us (e.g. if an individual completes an application or information request and provides additional personal information that was not requested)
- misdirected mail
- job applications not in response to an advertised job vacancy

The Legal Requirement:

If we receive unsolicited information, we must determine whether it is necessary for one or more of our activities or functions and:

- if it is not necessary, we must destroy or de-identify it
- if it is necessary, we must treat it as we would treat any unsolicited information, we have collected

How We Comply with This Obligation

If unsolicited personal information received by Investors Mutual Limited could not have been collected under APP 3 (Collection of Solicited Personal Information), we will destroy or de-identify the information as soon as practical, provided it is lawful and reasonable to do so.

It should be noted here that collection of personal information only occurs where a record is made of the information **(refer to What is a Record?).**

In the event that unsolicited personal information is received orally, it is important for employees to understand that this information will only be caught by the Privacy laws in the event that it is subsequently recorded.

It is the business's policy that employees do not record unsolicited personal information received during conversations, unless that information is relevant to the functions and activities of the business.

Principle 5: Notification of the Collection of Personal Information

The Legal Requirement:

At or before the time of collection (or if not practical, as soon as practical afterwards), Investors Mutual Limited must take reasonable steps to notify an individual about, or ensure an individual is aware of, certain matters concerning the purpose and circumstances of the collection of their personal information.

Information which we are required to provide to individuals includes:

- our business identity and contact details
- the circumstances of collection if the individual may be unaware that the information has been collected or the circumstances of collection
- details of the relevant law where the collection of personal information is required or authorised by law
- the purposes of collection
- the consequences if the personal information is not collected
- details of any other entities or types of entities to whom the collected information may be disclosed
- whether our organisation will disclose personal information to overseas recipients, and if practical, the countries in which those recipients are located

- information about Investors Mutual Limited's Privacy Policy which includes information on how to make a complaint and how an individual can access and seek correction of their personal information

It is important to note that Investors Mutual Limited is only required to take "reasonable steps" to inform people of such matters (noted above) that are "reasonable in the circumstances".

Deciding what is reasonable involves balancing the importance of the information to the individual and the time and cost to the business in providing that information. It would not be expected that we provide notification of matters that are considered to be obvious or likely to be known.

How We Comply with This obligation

We comply with our obligations with respect to the notification of collection of personal information through a combination of

- our Privacy Policy
- the use of Standardised Information Collection Forms, which incorporate a Privacy Collection Notice

Our Privacy Policy

Our Privacy Policy sets out how we manage personal information including:

- who we collect information from
- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use, and/or disclose personal information
- how an individual can access their personal information and seek a correction of the information
- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients, and if so, the countries in which those recipients are based

A copy of our Privacy Policy is published on our public website and made available on request.

Standardised Information Collection Forms

Where possible, Investors Mutual Limited has attempted to standardise the collection of personal information by using specifically designed forms (e.g. our Application Forms) which include a **Privacy Collection Notice.**

Principle 6: Use or Disclosure of Personal Information:

The Legal Requirement:

Use or Disclosure for a Primary Purpose

Investors Mutual Limited must only use or disclose personal information it holds for the primary purpose for which it was collected.

'Use' of personal information includes acts such as accessing the information, searching records that contain the information and transferring the information from one part of our business to another part or a related entity.

'Disclosure' of personal information includes any act that permits the information to become known outside Investors Mutual Limited and releases it from our effective control.

"Primary Purpose" is not a defined term, however, the context of the collection of information will more often than not identify the primary purpose of providing services in relation to the registered managed investment schemes that IML operate including complying with our customer identification obligations. The precise purpose, however, will depend on the circumstances.

Use and Disclosure for a Secondary Purpose

Investors Mutual Limited may only use or disclose personal information for a secondary purpose (i.e. any purpose other than the primary purpose) if one or more of the following circumstances exist:

- the individual has consented to a secondary use or disclosure

The individual would reasonably expect the use or disclosure of the personal information for the secondary purpose and the secondary purpose is related to the primary purpose in collection. In line with the individual's reasonable expectations, we will only use or disclose the personal information or part thereof, to the extent necessary for the secondary purpose.

In the case of sensitive information, the individual would reasonably expect the use or disclosure of the sensitive information for the secondary purpose and the secondary purpose is directly related to the primary purpose (i.e. it is closely associated with the primary purpose, even if it is not necessary to achieve the primary purpose).

A **Permitted General Situation** such as the following exists in relation to the use or disclosure:

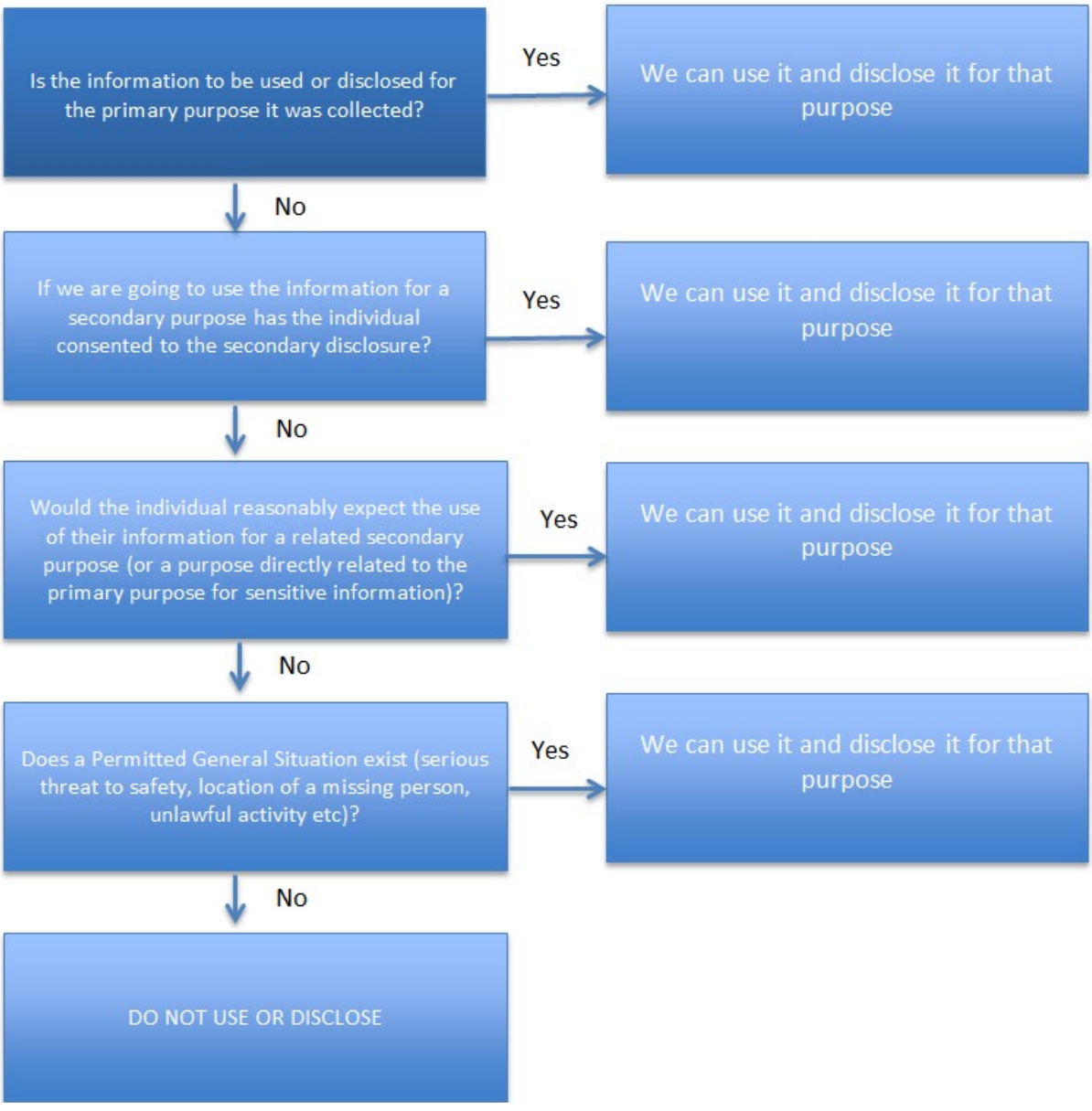
- where we reasonably believe that the use or disclosure is necessary to lessen or prevent a serious safety concern
- where we have reason to suspect that unlawful activity or misconduct of a serious nature is being, or has been engaged in

- where we believe the use or disclosure is necessary to assist in locating a missing person
- where the use or disclosure is reasonably necessary to establish, exercise, or defend a legal claim
- where it is reasonably necessary for confidential alternative dispute resolution process
- where it is necessary for a diplomatic or consular activity or for certain Defence Force activities
- it is authorised by law or court/tribunal order
- it is reasonably necessary for one or more law enforcement related activities

How We Comply with This Obligation

We comply with our obligations with respect to use and disclosure of personal information through a combination of:

- our Privacy Policy
- the use of Standardised Information Collection Forms that incorporates a Privacy Collection Notice
- by following guidelines outlined in the following diagram



The Legal Requirement:

Investors Mutual Limited must not use or disclose personal information for the purpose of direct marketing, unless one of the following situations exists:

A. Where we have collected personal information directly from the individual, and they would reasonably expect us to use or disclose the information for direct marketing, we provided a simple means for the individual to "opt out" of receiving direct marketing communications from us, and they have not done so.
B. Where we have collected personal information either directly from the individual, or from a third party, and the individual would not have a reasonable expectation that we would use it for direct marketing, we either:

- obtain the individual's consent; or
- if the information is "sensitive information", the individual has consented to its use

How We Comply with This Obligation

- we do not use sensitive information for direct marketing purposes unless we have the individual's consent to do so
- if we use an individual's personal information for the purpose of direct marketing (for example generating new business), in each direct marketing communication we include prominent statement allowing the individual to request not to receive direct marketing material. This is also known as 'opting out'
- in the event that we receive an "opt out" request, we comply with this request and update our databases accordingly

Principle 8: Cross-border Disclosure of Personal Information

The Legal Requirement:

Where Investors Mutual Limited discloses personal information to an overseas recipient, we are legally accountable if the overseas recipient mishandles the personal information, unless one of the following applies:

- the overseas recipient is subject to the laws of a country, or a binding scheme, that we reasonably believe to be substantially similar to the protections afforded to personal information under the 13 APPs and an individual can access mechanisms to enforce protections of the law or binding scheme.
- we have the individual's consent, after expressly informing them in a statement of the potential consequences of providing consent.
- a Permitted General Situation exists

When would we be likely to Disclose Information to an Overseas Recipient?

Examples of when we would be likely to disclose personal information to an overseas recipient include:

- publishing unsecured personal information using a 'cloud-based' computer storage service with servers based outside Australia

- sending emails or hardcopy documents containing personal information to an overseas recipient
- discussing personal information at an overseas meeting or with an overseas recipient over the phone and making record of it
- publishing personal information on the internet (e.g. on social media sites such as Facebook or Twitter) that is accessible by overseas recipients.
- providing personal information to an overseas contractor or service provider (such as a Custodian or Administrator)

Principle 9: Adoption, Use or Disclosure of Government-Related Identifiers

The Legal Requirement:

Investors Mutual Limited must not:

- use government related identifiers (such as their Medicare, Centrelink, Passport, Drivers Licence, or Tax File numbers) to identify an individual
- use or disclose a government related identifier, unless it is reasonably necessary to either verify the identity of the individual or is required by law

Note: A person's name and the Australian Business Number are not defined as government related identifiers under the Privacy Act.

How We Comply with This Obligation

We may use government related identifiers to identify individuals when required by law, such as under the AML/CTF Act and Rules.

We do not use government related identifiers to identify individuals. Our staff are unable to enter a government related identifier into a database and retrieve personal information based upon that identifier.

Where it is necessary for us to collect and hold a government related identifier of an individual, we do not use or disclose this personal information unless it is reasonably necessary.

Principle 10: Quality of Personal Information

The Legal Requirement:

Investors Mutual Limited must have practices, procedures and systems in place to ensure that the personal information we collect, use, hold, and/or disclose is accurate, up-to-date, complete, and relevant.

The rationale behind this requirement is to prevent situations where we may use or disclose inaccurate, incomplete, or out-of-date personal information.

How we Comply with This Obligation

We have established and effectively implemented practices, procedures and systems to ensure that the personal information we collect, use, hold, and/or disclose is accurate, up-to-date, complete, and relevant.

These practices, procedures, and systems include:

- ensuring personal information is collected and recorded in a consistent format, where possible, through the use of standardised forms and privacy collection notices
- ensuring updated or new personal information is promptly added to existing records
- identifying and correcting or destroying poor quality or incorrect personal information
- destroying or de-identifying personal information that is no longer required for the primary purpose for which it was collected whilst ensuring compliance with any record keeping obligations under the AML/CTF Act
- providing training to our staff outlining our expectations with respect to the management of personal information
- Ensuring that third parties collecting personal information have appropriate data quality collection/recording practices, procedures, and systems regularly reviewing our personal information management practices, procedures and systems.
- implementing risk-based systems and controls to determine whether and in what circumstances KYC information should be updated or verified in respect of our customers for ongoing customer due diligence purposes.

Principle 11: Security of Personal Information

The Legal Requirement:

Investors Mutual Limited must take active measures to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.

How we Comply with This Obligation

Securities Practices, Procedures, and Systems

Investors Mutual Limited has developed practices, procedures, and systems relating to the security of personal information we handle, which are designed to prevent the misuse, loss, inappropriate accessing, modification, or disclosure of personal information.

These practices, procedures and systems which have been developed having regard to the **Guide to Information Security** published by the Office of the Australian Commissioner (April 2013) include:

- appointment of designated individuals who are primarily responsible for managing and protecting the integrity of the personal information we collect. These individuals are allocated specific tasks to ensure our compliance and privacy laws and these tasks are monitored through online assurance questions.
- ensuring personal information (in particular financial information) that is stored in hard copy form, is stored securely
- the use of security and alarm systems to ensure the security of physical files and computer systems containing personal information
- the installation of up-to-date Information and Communications Technology (ICT) security software to protect the business' computer networks, websites, web-based applications and electronic devices from malicious software (or malware), computer viruses and other harmful programs and unauthorised access
- the use of passwords enabling only authorised persons to access the business' ICT systems on a need-to-know basis
- the regular monitoring and testing of our business' ICT security systems
- the back-up of personal information held on our ICT systems to protect against the loss of personal information

The implementation of policies that are designed to ensure that any staff who are required to take personal information outside the office or have personal information accessible through a laptop computer or mobile device, are required to ensure the maintenance of confidentiality (especially with respect to sensitive information). Refer to the following policies:

- Cyber Security Policy
- Social Media Usage Policy

IT Support & Usage

Managing Data Breaches

In the event of a breach of personal information, Investors Mutual Limited will:

- take immediate steps to contain the breach and undertake a preliminary assessment
- evaluate the risks for the individuals associated with the breach and asses what personal information is involved
- where there is a real risk of serious harm, notify the individuals involved as soon as possible, to enable them to avoid or mitigate harm. This includes providing a description of the breach, type of personal information involved, and recommend steps they should take to help mitigate against potential harm
- fully investigate the cause of the breach and make appropriate changes to policies and procedures
- notify the Office of the Australian Information Commissioner, law enforcement, and the organisations affected by the breach that Investors Mutual Limited is contractually required to notify

Destroying or De-Identifying Personal Information

If Investors Mutual Limited no longer requires personal information it holds, it will destroy or deidentify the information.

If held in hard copy form, the information is destroyed through a secure process of document destruction.

If held in hard copy form, steps are taken to irretrievably destroy the information or put it 'beyond use'.

If held by a third party, such as a cloud storage provider, our business will instruct the third party to delete the personal information and to verify that deletion has occurred.

Principle 12: Access to Personal Information

The Legal Requirement

Individuals have the right of access to any personal information we hold about them. There are some limited exceptions to this right of access including where access would:

- be unlawful
- pose a serious threat to the life or health of another individual
- unreasonably impact on the privacy of others
- require us to disclose evaluative information in connection with a commercially sensitive matter
- adversely impact an internal investigation into unlawful activities
- be considered frivolous or vexatious
- involve legally privileged information during legal proceedings
- where a request for access to personal information is made, we must respond within a reasonable amount of time.

If access is denied, we must give:

- written notice for the reasons for refusal (except where it would be unreasonable to do so)
- the mechanisms available to complain about the refusal

The Privacy Act allows us to impose a charge that is designed to cover costs however, we must disclose this charge to the individual upfront.

How we Comply with This Obligation

Requests for access to personal information are referred to our **Privacy Officer** who will consider each request on its merits, having consideration to the various exemptions with

respect to the rights of the individual, and respond appropriately within a reasonable timeframe.

Principle 13: Correction of Personal Information

The Legal Requirement

Investors Mutual Limited must take responsible steps to correct personal information where we become aware that the information we hold is inaccurate, out-of-date, incomplete, irrelevant or misleading, either as a result of our own internal activities, systems and procedures, or if we are requested to do so by an individual. An individual can request to access, review, delete, update or inquire about the information.

If we have disclosed information to another organisation, we must take responsible steps to notify the other organisation of any corrections we make where the individual has requested us to do so.

If an individual requests that a correction be made, and we refuse that request, we must provide written reasons for the refusal and information as to how the individual can complain about the refusal.

If we refuse a correction request, and the individual requests us to place with the information, a statement that the individual believes the information to be incorrect, we must take reasonable steps to do so in such a way that ensures that any users of the information are aware of the individual's position.

We must action corrections within a reasonable period (usually within 30 days) and we must not charge for making corrections. If you have any complaints about the dealings with your personal information, please contact our Privacy Officer. You may also refer the matter to the Privacy Commissioner with the Office of the Australian Information Commissioner at oaic.gov.au.

How We Comply with This Obligation

Investors Mutual Limited is committed to taking reasonable steps to ensure the personal information we hold is accurate, up-to-date, complete, relevant and not misleading, and we have established internal systems and procedures for correcting personal information. These Include:

- training staff to recognise the importance of maintaining up-to-date personal information
- effective database management including the investigation and correction of "bounced emails", "returned letters", and incorrect telephone numbers

Simple requests for correction of personal information will be dealt with directly by staff (e.g. a request to update a client's address or a contact telephone number).

Any correction requests that are potentially contentious are referred to our Privacy Officer who will consider each request on its merits.

In all cases where a correction request is made, Investors Mutual Limited will:

- respond in a timely manner (usually within 30 days)
- ensure any other entities the personal information was disclosed to are informed of the correction
- not charge the individual for making a request, correcting personal information or associating a statement
- give notice to an individual, including reasons and available complaint mechanisms, if the correction is refused

Transfers Between Related Entities

Under the Privacy Act, whilst all companies with an annual turnover exceeding $3 million must comply with the APPs, "related entities" (as defined by the Corporations Act 2001) are able to share and transfer personal information (but not sensitive information). In general terms, companies are related where they have a shared controlling interest.

This provision covering information transfers between related entities, highlights the fact that Investors Mutual Limited is not able to simply share information with other entities unless they are "related", or there is a reasonable expectation that this information would be shared for a secondary purpose. (Refer to APP6)

We have noted in our Privacy Policy that we may disclose personal information to unrelated entities such as:

- our Custodian and Investment Administrator
- our external IT Service Provider

Dealing with Privacy Questions and Complaints

Privacy inquiries or complaints are dealt with on a similar basis to any other inquiries and complaints we receive. Inquiries and complaints can arise verbally in writing.

Verbal Privacy Inquiry or Complaint

To ensure all verbal privacy enquiries or complaints received are managed appropriately, staff must record details of the enquiry or complaint through our Privacy Officer.

Handling a privacy complaint efficiently requires patience and skill to avoid an initial 'negative' situation becoming even more serious and escalating into a dispute.

Investors Mutual Limited's Complaints Handling and Dispute Resolution Policy have been purposely designed to minimise the potential for privacy complaints to turn into disputes. The Policy is available on www.iml.com.au.

Written Privacy Inquiry or Complaint

The following procedure is to be adopted where a written privacy inquiry or complaint is received.

All written privacy inquiries or complaints must immediately be forwarded to the Privacy Officer. The Privacy Officer will review the relevant correspondence and log details of the privacy inquiry or complaint in line with IML's Complaints Handling & Dispute Resolution Policy.

The person inquiring or complaining should be contacted by telephone (if possible) to acknowledge that we have received their inquiry or complaint and to obtain any additional information which may assist in resolving the matter quickly. Our guidelines relating to the management of verbal inquiries or complaints should be followed in this circumstance. If it is not possible to contact the person by telephone, additional information should be sought through appropriately worded written responses.

Privacy Complaints to the Office of the Australian Information Commissioner (OAIC)

If the person is not satisfied with the outcome of complaint, the person may refer to the matter to the OAIC. The person can send the complaint to the OAIC either by

1) Lodge an online Privacy Complaint Form available on the OAIC website (https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us)
2) Fax to +61 2 6123 5145
3) Mail to GPO Box 5288, Sydney NSW 2001

Privacy and the AML/CTF Act

Application of the Privacy Act to the AML/CTF Reporting Entities

When the AML/CTF Act was enacted, it amended the Privacy Act 1988, so that all businesses that are reporting entities for the purposes of the AML/CTF also became subject to the Privacy Act with respect to their obligations under the AML/CTF Act, notwithstanding that these businesses may have previously been exempt because they did not have an annual turnover of over $3 million.

How Much Information Should be Collected for the AML/CTF Purposes?

When collecting information for AML/CTF purposes, we should limit our collection to what is necessary based on the transaction and our AML/CTF obligations. For example, in many cases the collection of personal information may be limited to a minimum Know Your Customer (KYC) information. Additional information should not be collected in anticipation of a future use or need.

What Happens When Personal Information is Used or Disclosed

As a reporting entity we need to provide individuals with information about how their KYC information will be used and disclosed and the purpose of collection. We provide this information through our Privacy Policy which appears on our company website.

Can an Individual Correct Their KYC Information?

Yes. If requested to do so by an individual, we will take steps to rectify any personal information we have collected, where we are satisfied that the information is incorrect.

Can Sensitive Information Be Collected?

Some sensitive information may be collected for AML/CTF purposes, for example, membership of a professional association. Where this is necessary, the sensitive information must be collected with consent and stored securely to guard against improper use or disclosure.

What Are Our Obligations in Relation to Providing Individuals with Access to Their personal Information?

Access should be provided, unless there is a legitimate exception. For example, we may be able to deny access to a suspicious matter report lodged with AUSTRAC.

Changes to the Privacy Policy

We review the Policy annually. If we make material changes to the Policy, you will be notified via the ‘Disclosures & Policies' page of the IML website iml.com.au. Material changes are considered to include be:

- Changes to IML’s identity and contact details.
- Changes to the type of information and circumstances of collection.
- Changes to the purpose of collection, and
- Changes to the way IML use, process, store and disclose data.

Last updated: December 2023