PRIVACY POLICY

Purpose

This privacy policy sets out our information handling policies.

We are bound by the Australian Privacy Principles and the Notifiable Data Breaches (**NDB**) scheme under the Privacy Act.

This policy explains how we will collect, store, verify, use and disclose this information we hold and the conditions under which information may be accessed. It also explains our obligations for responding to data breaches.

Our privacy policy contained in our website (**Privacy Policy**) is also set out in this policy.

PROCEDURES – THE REPORTING OFFICER MUST TARGET THAT:	
1	The provisions of the Privacy Policy are reviewed semi-annually (March and September) to reflect any changes to our processes and systems in relation to how we handle personal information.
2	The contact details for the Licensee are updated if changes occur.
3	Data breach incident response, assessment and notification obligations are followed.
4	Training on the Privacy Policy and responding to data breaches is carried out in accordance with the training policy.

Privacy

We are bound by the Privacy Act, its Amendment (Enhancing Privacy Protection) Act, and its Privacy Amendment (Notifiable Data Breaches) Act, and we will protect your personal information in accordance with the Australian Privacy Principles (**APP**s). These principles govern how we can collect, use, hold and disclose your personal information, and how we respond when a data breach (including cyber and data security breaches) is likely to result in serious harm to any individuals whose personal information is involved in the breach.

What kinds of personal information do we collect and hold?

When you apply for an interest in any of our funds (**Funds**), we may collect information that is necessary to be able to provide you with an interest in a Fund. For instance, we may ask for identification information such as your name, address, and date of birth. Any unsolicited personal information we may collect will be promptly destroyed.

Why do we collect, hold, use and disclose personal information?

The main reason we collect, use, hold and disclose personal information is so we can service your request concerning a Fund. This may include:

- Checking your eligibility for the Fund;
- Providing you with the Fund; and
- Helping you manage your interests in the Fund.

How do we collect personal information?

We collect most personal information directly from you. Sometimes we collect personal information about you from other people such as publicly available sources of information.

How do we hold personal information?

Much of the personal information we hold will be stored electronically and securely by us at the offices of a Fund administrator. We use a range of security measures to protect the personal information we hold.

Who do we disclose your personal information to, and why?

Sometimes we may disclose your personal information to organisations outside the Licensee. For example, with the administrator of a Fund, so that it may perform its duties for a Fund and our services.

Who do we notify when there is a data breach of your personal information?

In accordance with the Notifiable Data Breaches (**NDB**) scheme under the Privacy Act, we are obliged to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm (these are referred to as 'eligible data breaches'). This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

In summary, subject to certain exemptions, the NDB scheme requires us to:

- Carry out a reasonable and expeditious assessment if there are reasonable grounds to suspect that there may have been an eligible data breach (and to take reasonable steps to complete that assessment within 30 days); and
- Make the prescribed notifications (to the Commissioner, and if practicable, to affected individuals) as soon as we are aware that there are reasonable grounds to believe that there has been an eligible data breach. The notifications must include a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

Do we disclose personal information overseas?

We may disclose your personal information to recipients located outside Australia. These entities may include our service providers.

Do we use or disclose personal information for marketing?

We may use your personal information to offer you products other than a Fund that we believe may interest you. We will not do this if you tell us not to.

If you don't want to receive marketing offers from us, please contact us on the details listed at 'Contact us' below.

Access to and correction of personal information

You can request access to the personal information we hold about you. You can also ask for corrections to be made. To do so, please contact us on the details listed at 'Contact us' (below).

Resolving your privacy concerns and complaints - your rights

If you are concerned about how your personal information is being handled or if you would like to make a complaint, please contact us on the details listed at 'Contact us' below.

If you are unhappy with our response, there are other bodies you can go to.

Contact us

If there is anything you would like to discuss, please contact us. If you have any questions or concerns about our privacy policy or practices, please contact us using one of the following methods:

- Email - enquiries@pellafunds.com
- Website contact form - www.pellafunds.com/contact
- Phone - +61 (02) 9188-1500

Operations Procedure

This is the operations procedure to follow if you suspect there is a data breach.

Maintain information governance and security - APP 1 and 11

We have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, that an entity holds.

Contain

Our first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess	Take remedial action
We will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If we have reasonable grounds to believe this is the case, we must notify the Commissioner. If we only have grounds to suspect that this is the case, we must conduct an assessment process. As part of the assessment, we should consider whether remedial action is possible.	Where possible, we should take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is

Organisations can develop their own procedures for conducting an assessment, OAIC suggests a three-stage process:

- Initiate: plan the assessment and assign a team or person
- Investigate: gather relevant information about the incident to determine what has occurred
- Evaluate: make an evidence-based decision whether serious harm is likely. OAIC recommends that this be documented.

We should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required, and we can process to the review stage.

NO **Is serious harm likely?** **YES**

Notify

Where serious harm is likely, we must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- Our identity and contact details
- A description of the breach
- The kind/s of information concerned
- Recommended steps for individuals

We must also notify affected individuals and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- Option 2: Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- Option 3: publish the statement on our website and publicise it
- We can provide further information in their notification, such as an apology and an explanation of what we are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to target the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

We should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australia Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.