Coolabah Capital
Wholesale fund manager for Smarter Money Investments

Smarter Money Investments™

Privacy Policy

28 February 2018

Applies to following entities, referred to as the "investment manager" as appropriate:

- Smarter Money Investments Pty Ltd (SMI) ACN 153555867
- Coolabah Capital Investments Pty Ltd (CCI) ACN 153327872
- Coolabah Capital Institutional Investments Pty Ltd (CCII) ACN 605806059

Applies to following funds and individually managed accounts (IMAs), referred to as "funds "or "portfolios":

- Smarter Money Fund, called Smarter Money Active Cash (SMAC), ARSN 154 023408
- Smarter Money Higher Income Fund (SMHI), ARSN 601 093485
- Smarter Money Long-Short Credit Fund (LSCF), ARSN 617 838 543
- CCI and CCII portfolios

1. Introduction and Objective

This document sets out our commitment in respect of personal information that we hold about our investors and clients ("clients") and what we do with that information. Our overarching objective is to ensure protection of all client personal information at all times.

Any personal information we collect about our clients will only be used for the purposes we have collected it, or as allowed under the relevant law. Our commitment in respect of personal information is to abide by the Australian Privacy Principles for the protection of personal information, as set out in the Privacy Act and any other relevant law.

1.1 Personal information

When we refer to personal information we mean information from which our client's identity is reasonably apparent. The personal information we hold about our clients may also include credit information. The kinds of personal information we may collect about our clients include their name, date of birth, address, account details, occupation, and any other information we may need to identify our clients.

Credit information is information which is used to assess our client's creditworthiness. *Registration information* is the information our clients provide in the course of registering for one of our funds or services. Registration information may include name, email address, address details, gender and date of birth. It includes additional information which our clients provide in the course of that relationship.

1.2 Why we collect personal information

We collect personal information during the investment application process and in order to comply with any relevant laws and regulations including:

- Anti-Money Laundering and Counter Terrorism Financing Act 2006;
- The Privacy Act 1988;
- The Corporations Act 2001;
- Any requirements or regulations under our Australian Financial Services License; and
- Any other requirements by regulators including ASIC.

We also confirm our obligation under Schedule 3 of the Privacy Act on National Privacy Principals – Collection which states "that an organization must not collect personal information unless the information is necessary for one or more of its functions or activities".

Noting the above, we however may be required to disclose our client's personal information in limited circumstances such as:

- To other organizations that are involved in managing or administering our client's investment such as third-party suppliers (Fund Administrators and Custodians);
- As required or authorized by or under law such as under the Anti-Money or Laundering and Counter Terrorism Financing Act 2006. This accords with principle 11 of the Privacy Act.

Prior to disclosing any of our client's personal information to another person or organization, we will take all reasonable steps to satisfy ourselves that:

a) The person or organization has a commitment to protecting our client's personal information at least equal to our commitment, or
b) Our client has consented to us in making the disclosure.

We may use cloud storage to store the personal information we hold about our clients. The cloud storage and the IT servers will be located within Australia and will always need to satisfy our internal requirements that all data stored is protected at all times.

2. Updating personal information
During the course of our relationship with our clients, we may ask our clients to inform us if any of their personal information has changed. We will generally rely on our clients to ensure the information we hold about our clients is accurate or complete.

3. Client access to, and updating, personal information
We will provide our clients with access to the personal information we hold about them. Our clients may request access to any of the personal information that we hold about them at any time. This accords with principle 6 of the Privacy Act.

4. Using government identifiers
If we collect government identifiers, such as tax file numbers or client's Australian Business or Company Number, we do not use or disclose this information other than required by law.

5. Safety and security of stored information
We will take reasonable steps to protect our client's personal information by storing it in a secure environment. We may store our client's personal information in paper and/or electronic form. We will also take reasonable steps to protect any personal information from misuse, loss and unauthorized access, modification or disclosure and this accords with principle 4 of the Privacy Act.

6. Using online services
When our clients access and interact with our website or online services, we may collect certain information about those visits. For example, in order to permit connection to our services, our servers may receive and record information about computer, device, and browser, including potentially IP address, browser type and other software or hardware information. If our clients access our services from a mobile or other device, we may collect a unique device identifier assigned to that device, geolocation data, or other transactional information from that device. Technologies may also be used to collect and store information such as pages our clients have visited, content viewed, search queries run and advertisements viewed in relation to our client's usage of our services and

other websites they have visited.

7. Information disclosure for merger or sale of business
If we sell all or part of our business or makes a sale or transfer of our assets or are otherwise involved in a merger or transfer of all or a material part of our business, we may transfer or disclose our client information to the party/parties involved in the transaction as part of that transaction and as part of any due diligence processes which take place in contemplation of a potential transaction.

8. Information disclosure for investor due diligence
Potential clients when performing operational due diligence on the investment manager may in the course of their diligence have access to our client list (but not their personal information) but we will require them to be bound by confidentiality.

9. Record Keeping
We will maintain records of our clients for a period of 7 years as required by law. This includes records with regard to the verification and identification of our clients.

10. Change in our Privacy Policy
We are constantly reviewing all of our policies and attempt to keep up to date with market expectations. Technology is constantly changing, as is the law and market place practices. As a consequence, we may change this privacy policy from time to time or as the need arises.

11. Data breach response plan
In August 2014, the **Office of the Australian Information Commissioner** ("**OAIC**") published a "**Data breach notification guide: A guide to handling personal information security breaches**". The investment manager's privacy policy observes the OAIC's guide by rolling out the **Data Breach Response Plan** outlined below.

On 1 September 2017, ASIC published its Corporate Plan which identified data security and privacy as one of its key challenges and areas to focus over the next 12 months. Specifically, ASIC is focused on how an organization ensures the security of the data, including personal information that it manages.

Why data breach notification is good privacy practice
Notifying clients when a data breach involves their personal information supports good privacy practice, for the following reasons:

• **Notification as a reasonable security safeguard** – As part of the obligation to keep personal information secure, notification may, in some circumstances, be a reasonable step in the protection of personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

• **Notification as openness about privacy practices** – Being open and transparent with clients about how personal information may be handled is recognised as a fundamental privacy principle. Part of being open about the handling of personal information may include telling clients when something goes wrong and explaining what has been done to try to avoid or remedy any actual or potential harm.

• **Notification as restoring control over personal information** – Where personal information has been compromised, notification can be essential in helping clients to regain control of that information. For example, where a client's identity details have been stolen, once notified, the client can take steps to regain control of their identity information by changing passwords or account numbers, or requesting the reissue of identifiers.

• **Notification as a means of rebuilding public trust** – Notification can be a way of demonstrating to the public that the investment manager takes the security of personal information seriously, and is

working to protect affected clients from the harms that could result from a data breach. Clients may be reassured to know that the investment manager's data breach response plan includes notifying them, the OAIC and relevant third parties.

Notification in appropriate circumstances is considered by the investment manager a good privacy practice, and in the interest of maintaining a community in which privacy is valued and respected.

Dealing with security breaches of client's data and information

(i) Cyber security breaches

If there has been a cyber security attack for example from:

- Databases containing client information being "hacked" into or otherwise illegally accessed by individuals outside of the investment manager.

that results in the client's data either being lost or compromised, **the following procedures should typically be followed by the Investment Manager:**

a) The Directors are promptly notified by either the Compliance Manager or an Executive Director and the Incident Response process is activated.
b) The Compliance Manager immediately engages the Cyber Security Consultant to implement a Remediation Plan.
c) The Cyber Security Consultant makes a recommendation about the activation of the disaster recovery plan and the physical relocation of full-time staff to home, or other offices and the availability and accessibility of its remote access services.
d) The Compliance Manager briefs its Cyber Security Insurer about the cyber security attack and initiate a claim under its policy for all claimable financial/other losses.
e) Depending on the severity of the cyber security attack, the Compliance Manager will notify as soon as reasonably practicable the following parties: external stakeholders including its key third party service providers, the impacted clients, ASIC, OAIC and other regulators where appropriate.
f) The Compliance Manager will also confirm that all the Investment Manager's regulatory, AFSL and contractual reporting and other obligations are fully met during and after the attack.
g) The Compliance Manager will maintain a register of cyber security attacks, the remediation plan, the financial and other impact and the insurance claims process.

(ii) Non-Cyber security breaches

If there has been a non-cyber security breach that results in the client's data either being lost or compromised, for example from:

- Lost or stolen laptops, removable storage devices, or paper records containing client information;
- Hard disk drives and other digital storage media;
- Employees accessing or disclosing client information outside the requirements or authorization of their employment;
- Paper records stolen from insecure recycling or garbage bins;
- The investment manager mistakenly providing client information to the person or party, for example by sending details out to the wrong physical or email address; and
- An individual deceiving the investment manager into improperly releasing the personal information of another person or client

depending on the severity of the breach and the timeliness/adequacy of the remediation

plan, the following procedures should typically be followed by the Investment Manager:

a) The Directors are promptly notified by either the Compliance Manager or an Executive Director and the Incident Response process is activated.
b) Depending on the severity of the breach, the Compliance Manager will notify as soon as reasonably practicable the following parties: external stakeholders including its key third party service providers, the impacted clients, ASIC, OAIC and other regulators where appropriate.
c) The Compliance Manager will also confirm that all the Investment Manager's regulatory, AFSL and contractual reporting and other obligations are fully met during and after the attack.
d) The Compliance Manager will maintain a register of client data breaches or losses, the remediation plan, the financial and other impact and the insurance claims process.