UNITY FUND SERVICES

Privacy Policy

Unity Fund Services

29 September 2025

PUBLIC

Table of Contents

1. Application of Policy

1.1. This policy applies to Unity Fund Services Pty Ltd (**UFS**) and its subsidiaries.

2. Purpose of Policy

2.1. Privacy is important and UFS is committed to managing personal information responsibly.

2.2. UFS considers having a documented approach to how it collects, secures, stores, uses and discloses personal information is important and this policy is designed:

(a) to assist in identifying the personal and sensitive information held by UFS;

(b) to describe how it collects, secures, stores, uses and discloses personal information;

(c) to describe UFS's approach to Notifiable Data Breaches; and

(d) to set out the role of the Privacy Officer.

3. What information does UFS collect?

3.1. Generally, UFS does not collect personal information (including sensitive information). Personal information is collected by its clients and their service providers but may be shared with UFS to enable UFS to provide services to its clients.

3.2. In providing its services, including establishing and administering a client engagement, UFS may collect or receive the following information:

(a) full name, date of birth, gender and contact details including telephone, address, e-mail and fax about officers, employees and agents or authorised signatories of the client; and

(b) full name, date of birth, gender and contact details including telephone, address, e-mail and fax about investors in its clients financial products or the beneficial owners of those products.

Sensitive Information

3.3. UFS will not generally collect sensitive information other than in respect of potential employees where pre-appointments check such as bankruptcy and criminal record may be performed.

3.4. Where OIG's Employee Handbook directs, UFS would reject the potential employee where an adverse finding is revealed. Where the potential employee is rejected, UFS will destroy the information collected when it is no longer legally obliged to hold it[1].

4. How do we collect and hold personal information?

4.1. In collecting personal information, UFS will:

[1] *Part 10 of the AML/CTF Act generally requires information to be held for 7 years.*

(a) disclose how it manages personal information in an open and transparent way;

(b) not collect personal information unless that information is reasonably necessary for the one or more of UFS's functions or activities;

(c) only collect information by lawful and fair means;

(d) only collect personal information from the individual unless it is unreasonable or impracticable to do so; and

(e) if it receives personal information that was not solicited, destroy that information.

4.2. While an individual or a Client is not required to provide UFS with their personal information or personal information relevant to the Client's investors, if they do not do so UFS may not be able to provide the Client the services the Client requires.

4.3. Where an individual does provide UFS with their personal information, they agree to their information being collected, held, used and disclosed as set out in this Privacy Policy. UFS may revise this Privacy Policy and will place the revised Privacy Policy on the its website or otherwise notifying individuals of the change.

4.4. UFS may collect personal information in various ways including by emails or on-boarding materials or other documents, telephone, email, letters or other correspondence and from websites and other social media channels. Wherever practicable, UFS will collect information about individuals from them directly.

4.5. However, it may be necessary at times to collect information about individual from other external sources, such as:

(a) a service provider, such as a registry service provider or investment manager;

(b) a financial adviser or broker;

(c) an online application provider;

(d) authorised representatives, such as executors or administrators; and

(e) identification verification service providers.

UFS Website

4.6. If an individual uses an UFS website our web server (i.e. the computers that house our website) it has the capacity to collect the following types of information for statistical purposes:

(a) the number of users who visit the website;

(b) the number of pages viewed; and

(c) traffic patterns.

4.7. This is anonymous statistical data and no attempt is made to identify users or their browsing activities. This data is used only to evaluate UFS's website performance and to improve the content UFS displays to the audience.

4.8. Other information, such as browser type, is included in a 'cookie' that is sent to the user's computer when they complete certain tasks on UFS website. A cookie contains bits of

information that enables UFS servers to identify and interact efficiently with user's computer. Cookies are designed to provide a better, more customised website experience, and to make it easier for users to use UFS's website. Individual can configure their computer to accept or reject cookies.

5. What does UFS use personal information for?

5.1. UFS generally only uses and discloses information for the purpose for which it was disclosed or related purposes which would reasonably be expected. Those purposes include:

(a) to establish and administer client engagements or other relationships with UFS;

(b) to assist Clients to administer their products and provide services to the Client's investors;

(c) for communication purposes including surveys and questionnaires;

(d) to comply with UFS's record-keeping, reporting, and tax obligations;

(e) to comply with other legal obligations such as laws that may require UFS or their Client to "know your customer" or to report on tax compliance;

(f) to protect legal rights and to prevent fraud and abuse;

(g) for quality assurance and training purposes; and

(h) to assist a Client to handle any relevant enquiries or complaints.

5.2. UFS may be required by law to disclose personal information. For instance, UFS may be required to provide details to:

(a) Australian Government regulators such as the Australian Securities and Investments Commission or the Australian Tax Office and to other regulatory or government entities;

(b) as required by a court order (including in Family Law matters); and

(c) other regulatory or governmental entities outside of Australia.

5.3. To meet Client needs it may be necessary for UFS to release or provide access to external service providers to personal information held by it, for instance:

(a) to any organisations involved in providing, managing or administering UFS's Client's products, systems, or services such as investment managers, custodians, registries, mail houses and software and information technology providers;

(b) to auditors, consultants and other professional advisers;

(c) to appropriate advisers, such as financial, legal, or other consultancy services;

(d) to other fund administrators where the Client has requested UFS retire in their favour;

(e) to authorities investigating (or who could potentially investigate) alleged fraudulent or suspicious transactions in relation to a Client or an individual's investment in that Client or a product offered by that client.

5.4. Information about an individual or individual's dealings with UFS is not and will not be sold to any other company, individual, or group.

6. Accessing and Amending Personal Information

6.1. Individuals may request access to any personal information UFS holds about them. Generally, if it is incorrect, UFS will correct it at their request.

6.2. An individual's right to access is subject to some exceptions allowed by law[2]. Where they are able to, UFS will notify individuals of the basis for any denial of access to their personal information.

7. Protection and storage of Personal Information

7.1. All personal information UFS collect will be held securely and in accordance with this Privacy Policy.

7.2. Personal information collected is protected from unauthorised access through the use of secure passwords, user logins or other security procedures. Developments in security and encryption technology are reviewed regularly.

7.3. Where necessary, UFS reminds that Internet is an insecure medium.

8. Will information be sent overseas?

8.1. We do not anticipate that we will need to disclose information to overseas recipients other than UFS staff located in Vietnam and the Philippines. These UFS Staff members have contracted to abide by Australian Privacy Law and operate in an environment that is ISO 27001 (Data Security Management Systems) compliant.

8.2. UFS will take reasonable steps to ensure that any overseas recipient will deal with any personal information in a way that is consistent with the APPs.

9. Making UFS's Privacy Policy available

9.1. UFS will make its Privacy Policy available on its website and will send a printed version free of charge to those who request it[3].

9.2. UFS's Privacy Policy is available from UFS free of charge through:

(a) downloading a copy in document format from UFS website unityfundservices.com.au;

(b) requesting a copy be emailed by emailing a request to enquiries@unityfundservices.com.au;

(c) telephoning us and request a copy be mailed or emailed by calling (02) 8277 0070 (+612 8277 0070 for international callers); or

---

[2] For example, UFS may deny access where the information is the subject of a suspicious matter report made to AUSTRAC. Under s.41 of the AML/CTF Act it is a criminal offence to tip-off the customer that UFS considers a transaction as suspicious or as informed AUSTRAC of its suspicions.

[3] The APPs, particularly APP 5, requires UFS, as an APP entity to take such steps as are reasonable in the circumstances to make the UFS Privacy Policy available.

(d) writing to UFS and request a copy be mailed or emailed using UFS's postal address PO Box R1471, Royal Exchange NSW 1225.

9.3. If a copy of this Privacy Policy is requested in a particular format (for example, on audio disc) please contact UFS at the telephone number or postal address set out above and UFS will accommodate any reasonable request.

10. Complaints

10.1. If an individual has a complaint about the manner in which UFS has collected, held, used, disclosed, kept, or given people access to their personal information, they may complain to UFS by phone, email, letter or in person using the details in clause 9.2 above. The individual will need to provide UFS with sufficient details regarding their complaint and during the investigation phase, UFS may ask complainants to provide additional information.

10.2. Complaints will be referred to UFS's Privacy Officer who will investigate and then determine the steps UFS will take to resolve the complaint.

10.3. UFS will notify complainants in writing of UFS's determination, generally within 30 days. If the complainant is not satisfied with UFS's determination or does not receive a response within 30 days, the complainant can contact UFS to discuss their concerns and they can refer the complaint to the Office of the Australian Information Commissioner at www.oaic.gov.au.

11. Notifiable Data Breach

11.1. A Data Breach occurs when either personal information or sensitive information is lost or subjected to unauthorised access, modification, use of disclosure or other misuse or interference.

11.2. The data breaches can be caused or exacerbated by a range of factors, affect different types of personal information or sensitive information and give rise to a range of actual or potential harms to individuals, organisations and government agencies.

11.3. The data breaches are required to be assessed and reported under this Privacy Policy, the Breach and Incident Handling Policy and UFS's Data Breach Response Plan.

11.4. UFS's Data Breach Response Plan assists UFS in managing a data breach. The plan forms part of UFS's incident and breach reporting process but sets out a specific framework of procedures and lines of authority for UFS staff in the event of a data breach or suspected data breach.

11.5. If the unauthorised access, disclosure or loss of personal information is likely to cause serious harm to one or more individuals and the likely risk of serious harm has not been prevented by remedial action, we will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable. The notification will include our identity and contact details, a description of the incident, the kind/s of information concerned and any recommended steps for affected individuals.

12. Privacy Officer

12.1. UFS is part of the One Investment Group (OIG) and OIG has appointed a Privacy Officer to be

the first point of contact in OIG when privacy issues arise either internally or externally.

12.2. The Privacy Officer is responsible for:

(a) developing and implementing a privacy policy that suits OIG's business and complies with the law;

(b) ensuring that the OIG Privacy Policy and procedures are fully implemented and working effectively; and

(c) reporting to the board of OIG any breach of the OIG Privacy Policy.

13. Training and Compliance

13.1. The implementation of (including training on) and monitoring of compliance with this policy is undertaken in accordance with *Risk Management Framework*.

13.2. Compliance with this policy is mandatory and any actual non-compliance must be reported and assessed through the normal incident/ breach reporting process. Any deliberate act of non-compliance by any employee may result in disciplinary action.

14. Review of Policy

14.1. This policy will be reviewed at the intervals and in the manner described in the *Risk Management Framework*.

15. Other Relevant OIG Policies

15.1. In addition to the *Risk Management Framework*, other UFS relevant policies are:

(a) *Breach and Incident Handling Policy;*

(b) *IT Policy and Information Security Management Systems Framework;*

(c) *Employee Handbook; and*

(d) *Data Breach Response Plan.*

16. Dictionary and Interpretation

16.1. In this policy, a reference to a person performing an act, for example UFS Senior Manager, that person may delegate the performance of the relevant act to another, for example UFS Manager provided they adequately supervise their delegate.

16.2. In addition to the terms defined in the Compliance Management Systems Framework, when used in this policy, the following capitalised terms have the meanings set out below:

Term	Meaning
AML/CTF Act	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
AML/CTF Rules	Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007

Term	Meaning
APPs	The Australian Privacy Principles set out in the Privacy Act
Application Form	An application form or other request to invest in a fund operated by UFS or other method of providing its registry service provider with personal information.
NDB Act	Privacy Amendment (Notifiable Data Breaches) Act 2017
OAIC	Office of the Australian Information Commissioner
Personal Information	Information or an opinion (including information or an opinion forming part of a data base, 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. Personal information includes credit card details, information gathered on websites and mobile telephone numbers linked to user names and mailing lists.
Privacy Act	Privacy Act 1988, as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 including the APPs.
Sensitive Information	Is a subset of personal information and includes information or an opinion about a person's racial or ethnic origin, political or religious belief, philosophical beliefs, membership of professional or trade associations or unions, sexual preferences and practices and criminal record. It also includes health information and genetic information about an individual that is not otherwise health information.