SUPER FUND SERVICES AUSTRALIA

Privacy Statement

SFSA takes its obligations to protect privacy seriously and all personal information will be treated as strictly confidential at all times. However, in line with modern business practices and legal requirements SFSA may need to disclose information related to the Trustees, Members and/or SMSF fund affairs to organisations outside SFSA. Other organisations to which we disclose information may include:

a) legal practitioners e.g. for the purposes of preparing the Trust Deed and/or establishing a Trustee Company;
b) registered SMSF Auditors for compliance and auditing purposes;
c) information technology service providers to protect, maintain, review and develop our business systems, procedures and infrastructure including testing or upgrading our computer systems, electronic data backup and disaster recovery planning;
d) financial services technology providers who may collect, store and use this information to provide the most efficient, effective and accessible services via secure web-based software platforms. Some of these service providers may use servers that are located overseas;
e) government and regulatory authorities including Centrelink, DVA, ATO, ASIC and APRA in order to perform the services as set out in this Agreement or as required/authorised by law; and
f) professional advisers, including advisers/agents, accountants or legal advisers as authorised by the Trustee.

In addition, SFSA employees and external service providers/contractors are obliged to respect the confidentiality of any personal information held by SFSA through contractual arrangements. Rigorous due diligence procedures are carried out before SFSA enters into any new arrangement that may require disclosure of personal information, and for external service providers this includes ensuring appropriate privacy measures including physical and virtual security measures are in place to protect the confidentiality of any personal information and for the application of the Australian Privacy Principles.

Personal information will be stored on our computer database. All electronic information is protected through the use of a variety of computer and network security measures including user identifiers, permission levels and access passwords. This information is backed up regularly and stored securely off site.

Certain technology service providers that we utilise e.g. cloud-based data storage, technology and/or software providers, may store information across multiple countries. These include data and file storage providers, accounting and financial software service providers and back-up storage providers whose infrastructure is held in Australia, Canada, New Zealand, Europe, United Kingdom and the US. Where this is the case we take all reasonable precautions to ensure the information is protected including strict contractual arrangements regarding the confidentiality, use, access and security of the information stored. All providers are vetted to ensure they are compliant with all privacy regulations where they operate, for example the General Data Protection Regulations (GDPR) covering Europe (considered the toughest privacy and security law in the world) and the international ISO27001 standard for information security management systems, as relevant.