MCMAHON CLARKE

WINIM FUNDS MANAGEMENT PTY LIMITED

Privacy policy and procedures

10 February 2015

62 Charlotte St Brisbane Q 4000 GPO Box 1279 Brisbane Q 4001
T +61 7 3831 8999 **F** +61 7 3831 1121 **www.mcmahonclarke.com**

Contents

Introduction

1. Design and structure

1.1 *Design*

This Program is designed to—

(a) provide an overview of the Act, including the Australian Privacy Principles, and the information it protects

(b) describe personal and sensitive information

(c) describe how the Act and the Australian Privacy Principles apply to WFM

(d) set out the role of the Privacy Officer, and

(e) set out the practices, procedures and systems WFM must implement and maintain to ensure it complies with its obligations under the Act and the Australian Privacy Principles.

1.2 *Structure*

This Program is made up of two parts, as follows:

(a) Part A—Part A of this Program explains the application of the Act and Australian Privacy Principles to WFM's business, and sets out the role and responsibilities of the Privacy Officer.

(b) Part B—Part B of this Program contains practices, procedures and systems to ensure WFM complies with its obligations under the Act.

Part A—Application of the Act and the role and responsibilities of the Privacy Officer

2. Act and Australian Privacy Principles

2.1 *Objects of the Act*

The objectives of the Act include to promote the protection of the privacy of individuals and the responsible and transparent handling of Personal Information by the entities it applies to, as well as to provide a means for individuals to complain about an alleged interference with their privacy.

2.2 *Australian Privacy Principles*

(a) The Australian Privacy Principles are set out in Schedule 1 to the Act, and regulate the collection, security, storage, use and disclosure of personal information.

(b) The Australian Privacy Principles represent the minimum standards of privacy protection policy that must be adopted by the entities to which they apply.

(c) The OAIC has published a summary of the Australian Privacy Principles, which is set out in Schedule 4—Summary of the Australian Privacy Principles.

2.3 *Privacy codes*

(a) Under the Act, the Commissioner can approve and register enforceable codes which are developed by entities on their own initiative, developed on request from the Commissioner, or developed by the Commissioner directly. An APP Code sets out how one or more of the APPs are to be applied or complied with any APP Entities that are bound by the APP Code.

(b) As at the date of adoption of this Program, there are no APP Codes which bind WFM.

(c) If the Commissioner includes an APP Code on the Codes Register which binds WFM, then WFM must update and amend this Program to include policies and procedures designed to ensure WFM complies with its obligations under the applicable APP Code.

3. Personal Information and Sensitive Information

3.1 *Personal Information*

(a) The Act protects Personal Information, which is defined as information or an opinion about an identified (or reasonably identifiable) individual, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

(b) Personal Information means information or an opinion about an identified individual. It includes credit card details, information gathered on websites and mobile telephone numbers linked to user names and mailing lists.

3.2 *Sensitive Information*

The Act provides extra protection for Sensitive Information, which is defined to mean—

(a) personal information that is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record

(b) health information about an individual

(c) genetic information about an individual that is not otherwise health information

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or

(e) biometric templates.

4. Application of the Australian Privacy Principles

4.1 *APP Entities*

The Australian Privacy Principles apply to APP Entities, which include Agencies and Organisations.

4.2 *Organisation*

(a) For the purposes of the Act, an Organisation means an individual, body corporate, partnership, trust or any other unincorporated association, that is not (amongst other things) a Small Business Operator.

(b) A legal person is taken to be a different Organisation in each of their different capacities. For example, a body corporate (such as WFM) may be an Organisation in its personal capacity as well as in its capacity as the trustee of one or more trusts. Further, a trustee is taken to be a different Organisation for each trust for which it acts as trustee.

4.3 *Small Business Operator exception*

(a) A Small Business Operator, which is deemed not to be an Organisation for the purposes of the Act, is an individual, body corporate, partnership, unincorporated association or trust that—

(i) carries on one or more Small Businesses, and

(ii) does not carry on a business that is not a Small Business.

(b) However, a body corporate is not a Small Business Operator if it is related to a body corporate that carries on a business that is not a Small Business.

(c) A business is a Small Business at a time in a financial year if its Annual Turnover for the previous financial year was $3,000,000 or less. However, if the business is a new business and there was no time in the previous financial year when the business was carried on, the business is a Small Business at the test time only if its Annual Turnover for the current year is $3,000,000 or less.

4.4 *Small Business Operators which are Reporting Entities are treated as an Organisation for the purposes of the Act*

If a Small Business Operator is a Reporting Entity (or an authorised agent of a Reporting Entity) because of anything done in the course of a Small Business carried on by the Small Business Operator, then the Act applies as if the Small Business Operator were an Organisation (with any prescribed modifications) to the activities carried on by the Small Business Operator for the purposes of, or in connection with, activities relating to the AML/CTF Act or AML/CTF Rules.

5. Application of the Australian Privacy Principles to WFM

(a) As WFM is a Reporting Entity under the AML/CTF Act as it is an issuer of interests in managed investment schemes, WFM is required to comply with the Act, including the Australian Privacy Principles, in relation to the activities carried out by it in relation to the AML/CTF Act and its associated rules and regulations.

(b) If at any time WFM is not a Small Business Operator, then the Australian Privacy Principles apply to all activities or functions performed by WFM.

6. Appointment of Privacy Officer

(a) The Board may at its absolute discretion appoint or employ any person to be its Privacy Officer.

(b) Until determined otherwise by the Board, Fiona Dixon is appointed as the Privacy Officer.

(c) The Privacy Officer is the first point of contact when privacy issues arise either internally or externally.

(d) The Privacy Officer is responsible for—

(i) ensuring this Program complies with the law on an ongoing basis

(ii) ensuring that this Program and its procedures are fully implemented and working effectively

(iii) ensuring all activities to be performed by WFM under this Program are performed in accordance with this program, and

(iv) reporting any breach of this Program to the Board.

7. Monitoring of compliance

(a) The implementation and monitoring of compliance with this Program and the Act is undertaken by the Privacy Officer.

(b) The Privacy Officer must report to the Board at least once every 12 months as to WFM's compliance with this Program and the Act.

8. Review of this Program

8.1 *Annual Review*

(a) The Privacy Officer must review this Program at least once every 12 months, and whenever there is a significant change in the law which may affect the substance of this Program, including an amendment of the Act and the AML/CTF Act and the AML/CTF Rules.

(b) In addition, the Privacy Officer must review and update the compliance procedures contained in this Program as frequently as required, such as where it becomes apparent that a certain procedure is inadequate or inappropriate.

(c) A report of the review made by the Privacy Officer, and any recommendations, must be tabled at the next meeting of the Board after the report is completed.

8.2 *Consultation and Participation*

All senior managers of WFM must be invited by the Privacy Officer to assist in the review process.

Part B—Compliance procedures

9. Obligation and purpose

9.1 *Obligation to comply with the Australian Privacy Principles*

WFM is prohibited from doing an act, or engaging in a practice, that breaches an Australian Privacy Principle.

9.2 *Purpose of Part B of this Program*

WFM must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its functions or activities that will—

(a) ensure it complies with the Australian Privacy Principles, and

(b) enable it to deal with inquiries or complaints from individuals about its compliance with the Australian Privacy Principles.

The purpose of Part B of this Program is to set out WFM's practices, procedures and systems to ensure it complies with its obligations under the Act.

10. Privacy Policy

10.1 *Obligation to have a Privacy Policy*

WFM is required to have a clearly expressed and up-to-date Privacy Policy describing how it manages Personal Information.

10.2 *Content of WFM's Privacy Policy*

WFM's must ensure its Privacy Policy contains information relating to—

(a) the kinds of Personal Information WFM collects and holds

(b) how WFM collects and holds Personal Information

(c) the purposes for which WFM collects, holds, uses and discloses Personal Information

(d) how an individual may access Personal Information about the individual that is held by WFM and seek the correction of such information

(e) how an individual may complain about a breach of the Australian Privacy Principles, and how WFM will deal with such a complaint, and

(f) whether WFM is likely to disclose Personal Information to overseas recipients, and if so, then the countries in which such recipients are likely to be located (if it is practicable to specify those countries).

10.3 *Availability of WFM's Privacy Policy*

(a) WFM is required to take such steps as are reasonable in the circumstances to make the Privacy Policy available free of charge, and in such form as is appropriate.

(b) WFM's must ensure the Privacy Policy is available at all times—

(i) on its website, which is www.winim.com.au, and

(ii) is available in hard copy to any person requesting it free of charge.

(c) If a person or body request a copy of the Privacy Policy in a particular form, then WFM must take such steps as are reasonable in the circumstances to give the person or body a copy of the Privacy Policy in that form. For example, if a person requests an audio or braille copy of the Privacy Policy, then WFM must consider whether it is possible for WFM to satisfy this request at the time and whether it is reasonable in the circumstances for it to do so.

(d) WFM must ensure information on the availability of the Privacy Policy upon request and how it may be accessed is contained in all offer or disclosure documents in accordance with this clause 10.3.

10.4 *Adoption of WFM's Privacy Policy*

As at the date of adoption of this Program, WFM has adopted as its Privacy Policy and as the statement of this Program the terms sets out in Schedule 2—Privacy Policy.

10.5 *Statements in offer and disclosure documents*

(a) WFM must ensure all offer and disclosure documents offered or made available by it contains—

(i) a statement as to the availability of and access to the Privacy Policy

(ii) a general statement as to the substantial aspects of the Privacy Policy that may impact on investors in the product, and

(iii) a general statement as to the obligations of WFM in relation to the collection and handling of Personal Information.

(b) A pro forma statement for inclusion in WFM's offer and disclosure documents is contained in Schedule 3—Privacy statement. This statement must only be amended for inclusion in an offer or disclosure document to the extent it is necessary to accommodate the features of the relevant product, and must not be substantially amended without the written approval of the Board.

10.6 *Reviewing of the Privacy Policy*

(a) WFM must review the Privacy Policy whenever significant changes in the law occur, and at least annually.

(b) WFM must review the Privacy Policy whenever this Program is reviewed or amended to ensure the Privacy Policy adequately describes how WFM manages Personal Information.

11. Anonymity and pseudonymity

11.1 *Individuals must have the option of not identifying themselves*

Individuals must have the option of not identifying themselves, or using a pseudonym, when dealing with WFM in relation to a particular matter unless, in relation to that matter—

(a) WFM is required or authorised by or under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves, or

(b) it is impracticable for WFM to deal with individuals who have not identified themselves or who have used a pseudonym.

11.2 *Requirement to identify and verify Customers*

(a) In order to comply with its obligations as a Reporting Entity, WFM is required to identify its Customers before providing a Designated Services to them in accordance with its AML/CTF Program. WFM must not provide a Designated

Service to individuals who are unwilling to identify themselves if this means WFM will fail to comply with its obligations under the AML/CTF Act.

(b) WFM considers there are no circumstances in which it is possible to deal with a client of theirs without first identifying them and therefore this privacy principle does not apply to WFM

12. Collection of solicited Personal Information

12.1 *Prohibition on collection of Personal Information*

(a) WFM must not collect Personal Information unless the information is reasonably necessary for one or more of its functions or activities.

(b) WFM must ensure each document requesting Personal Information (for example, an application form for a financial product) only collects Personal Information which is required for the primary purpose for which it is being collected for, such as to comply with WFM's obligations under the AML/CTF Act.

(c) For the collection of Personal Information by any other means, WFM must ensure the primary purpose for the collection of the information is noted and that the collection of the information is reasonably necessary for the performance of its functions or activities.

12.2 *Prohibition on collection of Sensitive Information*

(a) WFM must not collect Sensitive Information about an individual unless—

(i) the individual consents to the collection of the information, and the information is reasonably necessary for one or more of its functions or activities

(ii) the collection of the information is required or authorised by or under an Australian law or a court or tribunal order, or

(iii) a Permitted General Situation exists in relation to the collection of the information by WFM.

(b) No Sensitive Information can be collected unless collection has been approved by the Privacy Officer.

12.3 *Collection of Personal Information*

(a) WFM must only collect Personal Information by lawful and fair means.

(b) WFM will not collect Personal Information from third parties unless it is unreasonable or impracticable for WFM to collect the information from the individual.

12.4 *Deemed unsolicited Personal Information*

All Personal Information received by WFM other than through WFM's formal information gathering process (e.g., through the use of application forms) is to be treated as unsolicited information for the purposes of this clause 12.

13. Dealing with unsolicited personal information

13.1 *Receipt of unsolicited personal information*

(a) If WFM receives Personal Information which it did not solicit, then WFM must, within a reasonable period after receiving the Personal Information, determine whether or not it could have collected the Personal Information in accordance with clause 12 of this Program.

(b) WFM may use or disclose the unsolicited Personal Information it received for the purposes of determining whether it could have collected the Personal Information in accordance with clause 12 of this Program.

13.2 *Destruction of unsolicited Personal Information*

(a) If WFM could not have collected the unsolicited Personal Information in accordance with clause 12 of this Program, and the information is not contained in a Commonwealth Record, then WFM must as soon as practicable, but only if it is lawful and reasonable to do so, destroy the Personal Information or ensure it is de-identified.

(b) If WFM could have collected the unsolicited Personal Information in accordance with clause 12 of this Program, then WFM must comply with clauses 14 to 22 of this Program in relation to the unsolicited Personal Information as if it had collected the Personal Information in accordance with clause 12 of this Program.

14. Notification of the collection of Personal Information

14.1 *Obligation to notify an individual of the collection of Personal Information*

At or before the time WFM collects Personal Information about an individual (or, if that is not practicable, as soon as practicable after WFM collects Personal Information), WFM must take such steps (if any) as are reasonable in the circumstances—

(a) to notify the individual of such matters referred to in clause 14.2 as are reasonable in the circumstances, or

(b) otherwise ensure the individual is aware of any such matters.

14.2 *Information which WFM must notify individuals*

For the purposes of clause 14.1, WFM must notify individuals of the following matters as is reasonable in the circumstances:

(a) WFM's identity (including its AFS licence number and ACN), and contact information (including the contact information of the Privacy Officer).

(b) If WFM collects Personal Information from someone other than the individual, or where the individual is not aware WFM has collected the Personal Information, then WFM must notify the individual of the fact WFM so collects, or has collected, the Personal Information and the circumstances in which it collected the Personal Information.

(c) If WFM is required to collect the Personal Information by or under an Australian law or a court or tribunal order, then the fact the collection is so required or authorised and the Australian law or details of the court or tribunal order which requires the collection.

(d) The purposes for which WFM collects the Personal Information from someone other than the individual.

(e) The main consequences (if any) for the individual if all or some of the Personal Information is not collected by WFM (such as the inability of WFM to perform a Designated Service without satisfying its obligations under the AML/CTF Act and AML/CTF Rules).

(f) Any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which WFM usually discloses Personal Information of the kind collected by WFM.

(g) That WFM's Privacy Policy contains information about how the individual may access the Personal Information about the individual held by WFM and how the individual can seek the correction of such information.

(h) That WFM's Privacy Policy contains information about how the individual may complain about a breach of the Australian Privacy Principles, and how WFM will deal with such a complaint.

(i) Whether WFM is likely to disclose the Personal Information to overseas recipients, and if so, then the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

14.3 *Provision of Privacy Policy*

To satisfy its obligation to individuals in relation to the notification of the collection of Personal Information, WFM must provide all individuals, at or before the time WFM collects Personal Information about an individual, with a copy of the Privacy Policy.

15. Use or disclosure of Personal Information

15.1 *Personal Information only to be used for a particular purpose*

(a) If WFM holds Personal Information about an individual that was collected for a particular purpose (for example, to meet its obligations under the AML/CTF Act), then WFM must not use or disclose the information for any other purpose unless the relevant individual has consented to the use or disclosure of the information, or in accordance with clause 15.3.

(b) WFM must ensure the primary purpose for the collection of Personal Information is apparent and brought to the attention of all individuals from whom Personal Information is being collected at the time of collection.

15.2 ***Use or disclosure of Personal Information for Direct Marketing***

This clause 15 does not apply to the use or disclosure by WFM of Personal Information for the purpose of Direct Marketing under clause 16 of this Program.

15.3 ***Reasonable expectation of secondary use or disclosure***

(a) However, WFM may use or disclose an individual's Personal Information for a purpose other than the particular purpose for which it was collected if—

(i) the individual would reasonably expect WFM to use or disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose

(ii) the use or disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order

(iii) a Permitted General Situation exists in relation to the use or disclosure of the information by WFM, or

(iv) WFM reasonably believes the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an Enforcement Body.

(b) If the Personal Information is also Sensitive Information, then the secondary purpose must be directly related to the primary purpose.

15.4 ***Collection of Personal Information from a related body corporate***

(a) If WFM collects Personal Information from a related body corporate, then the primary purpose for the collection of this Personal Information for the purpose of this clause 15 is the purpose for which the related body corporate collected the Personal Information.

(b) WFM must not use Personal Information collected from a related body corporate for a purpose other than the purpose for which the related body corporate collected the Personal Information, except in accordance with clauses 15.1 or 15.3 of this Program.

15.5 ***Written note of the use or disclosure***

If WFM uses or discloses Personal Information under clause 15.3(a)(iv), then WFM must make a written note of the use or disclosure.

15.6 ***Service providers***

Where WFM is to provide Personal Information to a service provider, WFM must ensure the contract of engagement requires the service provider to limit the use of the Personal Information to the primary purpose the information was collected, or otherwise in accordance with this clause 15.

16. Direct Marketing

16.1 *What is Direct Marketing?*

Direct Marketing is the practice of making unsolicited contact with an individual or organisation with a view to selling a product or service.

16.2 *Prohibition*

(a) If WFM holds Personal Information about an individual, then WFM must not use or disclose the Personal Information for the purpose of Direct Marketing except in accordance with clauses 16.3 or 16.4 of this Program.

(b) If the Privacy Officer or the Board authorises the use of Personal Information for Direct Marketing, then WFM must only use Personal Information for this purpose in accordance with this clause 16.

(c) If WFM intends to use Personal Information for Direct Marketing, then the Personal Information must be kept in electronic form and facilities must be in place to identify whether or not—

(i) it was made apparent and clearly stated in the form (or other means of collecting personal information) that the information may be used for Direct Marketing purposes, and

(ii) a request not to use the information for Direct Marketing purposes has been received from the individual.

16.3 *Exception—Personal Information other than Sensitive Information*

(a) WFM does not intend to use Personal Information for Direct Marketing. However, WFM may use or disclose Personal Information that is not Sensitive Information about an individual for the purpose of Direct Marketing if WFM collected the information from the individual and—

(i) the individual would reasonably expect WFM to use or disclose the information for that purpose

(ii) WFM provides a simple means by which the individual may easily request not to receive Direct Marketing communications, and

(iii) the individual has not made such a request to WFM.

(b) WFM may use or disclose Personal Information that is not Sensitive Information about an individual for the purpose of Direct Marketing if WFM—

(i) collected the information from—

A. the individual and the individual would not reasonably expect WFM to use or disclose the information for the purpose of Direct Marketing, or

B. someone other than the individual, and

(ii) either the individual has consented to the use or disclosure of the information for that purpose or it is impracticable for WFM to obtain consent from the individual to the use or disclosure of the information for that purpose

(iii) WFM provides a simple means by which the individual may easily request not to receive Direct Marketing communications

(iv) in each Direct Marketing communication with the individual, WFM includes a prominent statement that the individual may make such a request or otherwise draws the individual's attention to the fact the individual may make such a request, and

(v) the individual has not made a request to WFM not to receive Direct Marketing communications.

16.4 ***Exception—Consent to the use or disclosure of Sensitive Information***

Despite clause 16.1, WFM may use or disclose Sensitive Information about an individual for the purpose of Direct Marketing if the individual has consented to the use or disclosure of the information for that purpose.

16.5 ***Individual may request not to receive Direct Marketing communications***

(a) If WFM uses or discloses Personal Information about an individual for the purpose of its own Direct Marketing, or for the purpose of facilitating Direct Marketing by other Organisations, an individual may request—

(i) not to receive Direct Marketing communication from WFM

(ii) for WFM not to use or disclose the information for the purpose of facilitating Direct Marketing by other Organisations, and

(iii) request WFM to provide its source of the information.

(b) If an individual makes a request under paragraph (a) above, WFM must not charge the individual for the making of, or to give effect to, the request.

(c) WFM must give effect to all requests made under clause 16.5(a)(i) or 16.5(a)(ii) above within a reasonable period after the request is made.

(d) For the purpose of clause 16.5(a)(iii), WFM must notify the individual of its source within a reasonable period after the request is made, unless it is impracticable or unreasonable to do so.

16.6 ***Interaction with other legislation***

This clause 16 does not apply to the extent any of the following apply:

(a) *Do Not Call Register Act 2006*.

(b) *Spam Act 2003*.

(c) Any other legislation prescribed by the regulations.

17. Cross-border disclosure of Personal Information

17.1 *Ensuring compliance with the Australian Privacy Principles*

(a) Before WFM discloses Personal Information about an individual to an overseas recipient, WFM must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

(b) However, paragraph (a) above does not apply if—

(i) WFM reasonable believes that the overseas recipient is subject to a law or scheme which protects information in a substantially similar way to the Australian Privacy Principles, and there are mechanisms that the individual can access to take action to enforce that protection

(ii) WFM expressly informs the individual that if he or she consents to the disclosure of the information, WFM is not required to take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles, and the individual provides informed consent to the disclosure

(iii) the disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order, or

(iv) a Permitted General Situation (except items 4 or 5) exists in relation to the disclosure of the information by WFM.

17.2 *Breaches of the Australian Privacy Principles by an overseas recipient deemed to be breaches by WFM*

If WFM discloses Personal Information about an individual to an overseas recipient and paragraph 17.1(b) does not apply to the overseas recipient, then any act, or practice engaged in, by the overseas recipient which would be a breach of the Australian Privacy Principles if they applied to the overseas recipient, then WFM is deemed to have engaged in the act or practice and to have breached the Australian Privacy Principles.

17.3 *Overseas service providers*

(a) All contracts with overseas service providers must contain a privacy provision in a form approved by the Privacy Officer.

(b) WFM must not provide Personal Information to overseas service providers that are not located in an Approved Country.

(c) WFM must maintain and update the list of Approved Countries on an ongoing basis.

18. Adoption, use or disclosure of Government Related Identifiers

18.1 *Prohibition on adoption of a Government Related Identifier*

WFM must not adopt a Government Related Identifier of an individual as its own identifier of the individual unless required or authorised by or under an Australian law or a country or tribunal order.

18.2 *Collection, use and disclosure of Government Related Identifiers*

(a) WFM must not collect, use or disclose an individual's Government Related Identifier unless the collection, use or disclosure—

(i) is reasonably necessary to verify the identity of the individual for the purposes of WFM's activities or functions

(ii) is reasonably necessary to fulfil its obligations to an agency or a State or Territory authority

(iii) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court or tribunal order

(iv) a Permitted General Situation (except item 4 or 5) exists in relation to the use or disclosure of the identifier, or

(v) WFM reasonably believes that the use or disclosure of the identifier is reasonably necessary for activities conducted by, or on behalf of, an Enforcement Body.

(b) In accordance with paragraph 18.2(a), WFM may collect, use and disclose Government Related Identifiers for the purposes of identifying (and verifying) investors, such as collecting drivers licence numbers and passport numbers.

19. Quality and integrity of Personal Information

19.1 *Accuracy of Personal Information*

(a) WFM must take such steps (if any) as are reasonable in the circumstances to ensure the Personal Information it—

(i) collects is accurate, up-to-date and complete, and

(ii) uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

(b) WFM must only record Personal Information if it is collected from a form or other communication collected from the relevant person, or otherwise in accordance with clause 12 of this Program.

(c) WFM must review all Personal Information for any ambiguities and verify any information with the individual as required.

(d) When communicating with individuals after the initial collection of information, WFM must ensure individuals are identified as being who they say they are and confirming the Personal Information held by WFM in relation to the individual.

20. Security of Personal Information

20.1 *Storage and access*

(a) If an WFM holds Personal Information, then it must take such steps as are reasonable in the circumstances to protect the information—

(i) from misuse, interference and loss, and

(ii) from unauthorised access, modification or disclosure.

(b) All Personal Information held by WFM must be stored in password restricted computer databases that restrict access to authorised personnel. Hard copy records, if any, are to be kept in a locked filing cabinet with only key staff having access.

(c) Any hard copy records containing individual's Personal Information must not leave WFM's premises without the written authorisation of the Privacy Officer.

(d) Prior to engaging any service providers to provide offsite storage (whether electronic or otherwise), WFM must ensure the service provider has adequate and appropriate systems in place for the security of the Personal Information.

20.2 *Destruction of Personal Information*

(a) If Personal Information held by WFM is no longer needed for any purpose for which the information may be used or disclosed by it, and the information is not contained in a Commonwealth record or WFM is not required by or under an Australian law or a court or tribunal order to retain the information, then WFM must take such steps as are reasonable in the circumstances to destroy the information or to ensure the information is de-identified.

(b) When electronic data is due for destruction in accordance with this clause 20.2, WFM must ensure the relevant files are deleted in a manner that permanently destroys and deletes the Personal Information.

(c) Hard copy records due for destruction in accordance with this clause 20.2 must be shredded or otherwise destroyed in a manner approved by the Privacy Officer.

21. Access to Personal Information

21.1 *Requirement to give access*

If WFM holds Personal Information about an individual, WFM must, on request by the individual, give the individual access to the information, except in the circumstances set out in clause 21.2.

21.2 ***Exceptions***

WFM is not required to give the individual access to the Personal Information to the extent that—

(a) WFM reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety

(b) giving access would have an unreasonable impact on the privacy of other individuals

(c) the request for access is frivolous or vexatious

(d) the information relates to existing or anticipated legal proceedings between WFM and the individual, and would not be accessible by the process of discovery in those proceedings

(e) giving access would reveal the intentions of WFM in relation to negotiations with the individual in such a way as to prejudice those negotiations

(f) giving access would be unlawful

(g) denying access is required or authorised by or under an Australian law or a court or tribunal order

(h) WFM has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to WFM's functions or activities has been, is being or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an Enforcement Body, or

(j) giving access would reveal evaluative information generated by WFM in connection with a commercially sensitive decision-making process.

21.3 ***Handling of requests to access Personal Information***

WFM must respond to a request for access to Personal Information by an individual within 30 days after the request is made, and give access to the information in the manner requested by the individual if it is reasonable and practicable to do so.

21.4 ***Refusal to give access***

(a) If WFM refuses a request for access to the Personal Information under clause 21.2, or refuses to give access to the information in the manner requested by the individual, then WFM must take such steps (if any) as are reasonable in the circumstances to give access to the Personal Information in a way that meets the needs of WFM and the individual (such as through the use of a mutually agreed intermediary).

(b) If WFM refuses to give access to Personal Information under clause 21.2, or refuses to give access to the information in the manner requested by the individual, WFM must give the individual a written notice that sets out—

(i) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so

(ii) the mechanisms available to complain about the refusal, and

(iii) any other matter prescribed by the regulations.

(c) WFM must prepare and provide the written notice to the individual in accordance with clause 21.4(b) as soon as practicable, and in any event within 30 days after the decision to refuse access (or refuse to give access in the manner requested).

21.5 *Access charges*

(a) WFM must only charge individuals for administrative expenses for giving access to the Personal Information, and the charge must not be excessive.

(b) WFM must not charge any fees to an individual for making a request to access Personal Information.

22. Correction of Personal Information

22.1 *Obligation*

If WFM holds Personal Information about an individual, and WFM is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests the correction of the information, then WFM must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

22.2 *Notification of correction to third parties*

If WFM corrects Personal Information about an individual which it has previously disclosed to another APP Entity, and the individual requests WFM to notify the other APP Entity of the correction, then WFM must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

22.3 *Refusal to correct Personal Information*

(a) If WFM refuses to correct the Personal Information as requested by the individual, then WFM must give the individual a written notice that sets out—

(i) the reasons for the refusal (except to the extent that it would be unreasonable to do so)

(ii) the mechanisms available to the individual to complain about the refusal, and

(iii) any other matter prescribed by the regulations.

(b) WFM must make a determination as to whether or not the Personal Information is to be amended in accordance with the individual's request and notify the individual within 30 days of this determination.

(c) If a request to correct Personal Information is denied, then the individual must be made aware of the dispute resolution procedures available to them, such as by referring the complaint to the Office of the Australian Information Commissioner.

22.4 *Request to associate a statement*

If WFM refuses to correct the Personal Information as requested by the individual, and the individual requests WFM to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, then WFM must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

22.5 *Dealing with requests—Timing*

If an individual makes a request in accordance with clauses 22.1 and 22.4, then WFM must respond to the request within a reasonable period after the request is made.

22.6 *Dealing with requests—Access charges*

If an individual makes a request in accordance with clauses 22.1 and 22.4, then WFM must not charge the individual for making of the request, correcting the Personal Information, or associating the statement with the Personal Information.

23. Tax file number (TFN) collection

23.1 *General*

The *Privacy (Tax File Number) Rule 2015* (TFN Rule) regulates the collection, storage, use, disclosure, security and disposal of individuals' tax file number (TFN) information. The TFN Rule only applies to the TFN information of natural persons and does not apply to or regulate the collection of TFN information of other entities, such as companies and trusts.

A breach of the TFN Rule is an interference with privacy under the Privacy Act, and the unauthorised use or disclosure of TFNs can be an offence under the *Taxation Administration Act 1953* (TAA) and attract penalties including imprisonment and monetary fines. However, unlike the TFN Rule, the TAA protects all TFNs and not just those of individuals.

23.2 *Application*

WFM must ensure the requirements of the TFN Rule and this clause 23 are followed in relation to all customer types, not only natural persons.

23.3 *Collection of TFN information*

(a) An individual is not legally obliged to quote or provide WFM with their TFN.

(b) WFM must only request or collect TFN information from individuals for a purpose authorised by taxation law (e.g., withholding tax from an investor's income distributions).

(c) When requesting an individual's TFN, WFM must take reasonable steps to ensure—

(i) individuals are informed of the taxation law or superannuation law which authorises it to request or collect the TFN, and of the purpose for which the TFN is requested or collected

(ii) individuals are informed that declining to quote a TFN is not an offence, and about the consequences of declining to quote a TFN

(iii) the manner of collection does not unreasonably intrude on the individual's affairs, and

(iv) WFM only requests or collects information that is necessary and relevant to the purpose of collection under applicable taxation law.

(d) To comply with its obligations under the TFN Rule, as set out in paragraph (c), any document requesting an individual's TFN must include a statement in accordance with clause 23.7.

23.4 *Incidental collection*

(a) WFM may receive TFN information about individual without requesting it as part of its business from time to time. For example, documentation provided to enable WFM to meet its obligations under the AML/CTF Rules may contain an individual's TFN number.

(b) To reduce the likelihood of WFM receiving TFN information incidentally, in an application form, WFM may request that individuals to cross out, or otherwise render illegible, their TFN information prior to such documentation being provided to WFM.

(c) If WFM receives an individual's TFN information incidentally, then WFM must not use or disclose the TFN, and cross out, or otherwise render illegible, the TFN information as soon as possible.

23.5 *Use and storage of TFN information*

(a) WFM must only use or disclose TFN information for a purpose authorised by taxation law, or for the purpose of giving an individual any TFN information that WFM holds about that individual.

(b) WFM must take reasonable steps to—

(i) protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure, and

(ii) ensure that access to records containing TFN information is restricted to individuals who need to handle that information for taxation law purposes.

(c) Once TFN information is no longer required by law to be retained or necessary for a purpose under taxation law (including the administration of such law), WFM must securely destroy or permanently de-identify the information.

23.6 ***Training***

(a) To ensure all staff are aware of the need to protect individuals' privacy when handling TFN information, WFM must ensure a copy of this clause 23 or other document or statement containing the information set out in this clause 23, is provided to all staff.

(b) All staff who collect or access TFN information are aware of the—

(i) circumstances where TFN information may be collected

(ii) prohibitions on the use and disclosure of TFN information

(iii) need to protect individuals' privacy when handling TFN information, including under the TFN Rule and under the Privacy Act, and

(iv) the penalties or other sanctions that apply for breaching the TFN Rule or applicable laws relating to the handling of TFNs.

23.7 ***Disclosure***

WFM must ensure all offer and disclosure documents offered or made available by it, and any other document or statement which requests the provision of a TFN, contains the following pro forma statement or a statement of similar effect approved by the Board:

> *"The collection of tax file number information is authorised and its use and disclosure are strictly regulated by the tax law and the Privacy Act 1988 (Cth). It is not an offence if you choose not to quote your tax file number. However, if you do not provide your tax file number, then tax at the highest marginal rate plus the Medicare Levy will be deducted from your income distribution, unless you carry on an enterprise of investing and are entitled to quote your ABN as an alternative. Please contact us if you wish to quote your ABN instead.*
>
> *If you are exempt from quoting a tax file number, then you can claim that exemption rather than providing us with your tax file number. Information on the circumstances where an investor can claim an exemption from quoting a tax file number is available from the Australian Taxation Office's website."*

Schedule 1—Dictionary

Act	The *Privacy Act 1988* and its associated regulations, as amended from time to time.
AFS	Australian financial services.
Agencies	Defined in section 6 of the Act to include— (a) a Minister (b) a department (that is, an "agency" within the meaning of the *Public Service Act 1999*), and (c) other bodies established or appointed for a public purpose by or under a Commonwealth enactment.
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and its associated regulations as amended from time to time.
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* as amended from time to time.
Annual Turnover	The Annual Turnover of a business for a financial year is the total of the following that is earned in the year in the course of the business: (a) The proceeds of sales of goods and/or services. (b) Commission income. (c) Repair and service income. (d) Rent, leasing and hiring income. (e) Government bounties and subsidies. (f) Interest, royalties and dividends. (g) Other operating income.
APP Entities	Agencies and Organisations to which the Act applies.
Approved Country	An overseas country which satisfies clause 17.1(b)(i).
APPs or Australian Privacy Principles	The Australian Privacy Principles as contained in Schedule 1 of the Act.
APP Code	A written code of practice about information privacy made in accordance with the Act.
Board	WFM's board of directors.

Code Register	A register the Commissioner is required to keep under the Act, which includes APP Codes the Commissioner has decided to register under the Act.
Commissioner	The Information Commissioner within the meaning of the *Australian Information Commissioner Act 2010*.
Commonwealth Record	A Commonwealth record that is required to be readily available for the purposes of a Commonwealth institution, other than purposes under the *Archives Act 1983.*
Customer	A person to whom WFM is or will provide a Designated Service, such as a person applying to invest in the Fund or a person currently named in the Fund's register of members.
Designated Service	In relation to WFM, means the issue of interests in a managed investment scheme (the Fund) (item 35 of table 1 in section 6 of the AML/CTF Act) which occurs in the course of carrying out WFM's business.
Direct Marketing	Direct Marketing is the practice of making unsolicited contact with an individual or organisation with a view to selling a product or service.
Enforcement Body	An enforcement body is defined in section 6 of the Act and includes the Australian Federal Police and Australian Securities and Investment Commission.
Fund	The WINIM Funds Management Sylvan Road Trust, an unregistered mortgage investment scheme established by trust deed dated 11 November 2015, and such other managed investment schemes operated by WFM from time to time.
Government Related Identifier	A government related identifier of an individual means an identifier (such as a number, letter or symbol) used to identify the individual, other than the individual's name, ABN, or anything else prescribed by the regulations, that has been assigned by a government authority. Examples of government related identifiers include Medicare numbers, Centrelink Reference numbers, drivers licence numbers, and passport numbers.
OAIC	Office of the Australian Information Commissioner.

Organisations	Means— (a) an individual (b) a body corporate (c) partnership (d) any other unincorporated association, and (e) a trust.
Permitted General Situations	The items contained in Schedule 5—Permitted General Situations.
Personal Information	Has the meaning given by clause 3.1 of this Program.
Privacy Officer	The person appointed as the privacy officer in clause 6 of this Program.
Privacy Policy	The statement adopted by WFM which describes how it manages Personal Information, made in accordance with the Act and contained in Schedule 2—Privacy Policy.
Program	This privacy policies and procedures program, including all of its schedules.
Reporting Entity	A person who provides a Designated Service under the AML/CTF Act.
Sensitive Information	Has the meaning given by clause 3.2 of this Program.
Small Business	Has the meaning given by clause 4.3 of this Program.
Small Business Operator	Has the meaning given by clause 4.3 of this Program.
TFN Rule	The *Privacy (Tax File Number) Rule 2015*.
WFM or WINIM Funds Management Pty Limited	WINIM Funds Management Pty Limited ACN 600 668 399 AFS licence number 463394.

Schedule 2—Privacy Policy

WINIM Funds Management Pty Limited—Privacy Policy

This is the Privacy Policy for WINIM Funds Management Pty Limited ACN 600 668 399 (we, us or our), an Australian financial services licensee (number 463394) and operator of managed investment schemes.

Your privacy

We respect your privacy and we are committed to managing your personal information responsibly and in accordance with our legal obligations under the *Privacy Act 1988* (Privacy Act). The Privacy Act regulates the way we collect, use, disclose, keep secure, and give you access to, your personal information.

This Privacy Policy sets out the type of information we collect and how we collect, store, use and disclose your personal information.

You are not required to provide us with your personal information, but if you do not do so we may not be able to provide you with our products or services.

If you apply for or accept any of our products or services or otherwise provide us with your personal information, then you agree to your information being collected, held, used and disclosed as set out in this Privacy Policy.

Changes to our Privacy Policy

We may update and revise this Privacy Policy from time to time. The current version of our Privacy Policy can be accessed free of charge on our website, www.winim.com.au, or by contacting us on the details below. This version of our Privacy Policy was last updated in February 2015.

What kind of personal information do we collect and hold?

We will only collect personal information from you which is necessary for us to provide our financial products and services and to comply with our legal and regulatory obligations. In order to provide our products and services, we may collect the following information:

(a) Your full name, date of birth and contact details (including your residential address, e-mail address, and fax and telephone number).

(b) Information and documentation to verify your identity, such as a copy of your driver's licence or passport, to ensure compliance with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and/or other legislation and regulations regarding identification verification, and tax reporting and withholding.

(c) Your tax file number (as authorised under the tax laws and Privacy Act) and bank account details for the purpose of administering investor accounts and tax reporting and withholding.

(d) Investor contribution details and investment choice.

(e) Copies of any relevant trust deeds, partnership agreements or constitutions, which may be relevant to comply with the AML/CTF Act.

It may, on occasion also be necessary for us to obtain other details, including information relating to powers of attorney or for probate and estate administration.

How do we collect and hold your personal information?

Unless it is unreasonable or impractical for us to do so, we will collect your personal information from you directly, including—

(a) from you filling out application forms, such as an application form completed by you to acquire a financial product or receive other financial services from us

(b) through your use of our website

(c) from communications between you and our officers, employees and representatives (including communications conducted in person, over the phone, by email or otherwise), and

(d) from promotional and marketing activities undertaken by us, in which we request or otherwise receive personal information from you (such as from competitions organised by us).

However, we may also collect information about you from third parties, such as—

(a) your financial or other professional advisor or broker

(b) your authorised representatives, such as executors or administrators, and

(c) subject to your consent, identification verification service providers that we may engage to collect and verify personal information electronically.

Use of our website

We may use “cookies” to help us tailor our website to better suit your needs and improve our service. Cookies are small text files that are stored in your computer's memory and hard drive when you visit certain web pages. Cookies are used to enable websites to function or to provide information to the owners of a website.

We use cookies on this website for the following purposes:

(a) *Analytical purposes*—Analytical cookies allow us to recognise, measure and track visitors to the website. This helps us to improve and develop the way the website works, for example, by determining whether site visitors can find information easily, or by identifying the aspects of the site that are of the most interest to them.

(b) *Usage preferences*—Some of the cookies on the website are activated when visitors to our sites make a choice about their usage of the site. Our website then ‘remembers' the settings preferences of the user concerned. This allows us to tailor aspects of the site to the individual user.

(c) *Terms and conditions*—We use cookies on the website to record when a site visitor has seen a policy, such as this one, or provided consent, such as consent to the terms and conditions on our website. This helps to improve the user's experience of the site – for example, it avoids a user from repeatedly being asked to consent to the same terms.

(d) *Session management*—The software that runs the website uses cookies for technical purposes needed by the internal workings of our servers. For instance, we use cookies to distribute requests among multiple servers, authenticate users and determine what features of the site they can access, verify the origin of requests, keep track of information about a user's session and determine which options or pages to display in order for the site to function.

(e) *Functional purposes*—Functional purpose cookies store information that is needed by our applications to process and operate. For example, where transactions or requests within an application involve multiple workflow stages, cookies are used to store the information from each stage temporarily, in order to facilitate completion of the overall transaction or request.

Storage and security

All personal information we collect will be held securely and in accordance with this Privacy Policy. We will protect your personal information and prevent unauthorised access through the use of secure passwords, user logins, or other security procedures, including firewalls and anti-virus technology.

However, we cannot provide any assurance regarding the security of information transmitted to us online, as the internet is inherently insecure. Nor can we guarantee the supply of information to us from you will not be intercepted. Information you transmit to us online is at your own risk.

Purposes for which we collect, hold, use and disclose personal information

We will only use and disclose your personal information for the purpose of providing our financial products and services to you. We may use and disclose your personal information to—

(a) assess your application and establish and administer your investment

(b) communicate with you (or your advisor) in relation to your investment

(c) comply with our legal, regulatory and other obligations, including our reporting and recording keeping obligations

(d) improve the quality of our services and for training purposes

(e) assist with the administrative, marketing (including direct marketing), planning, product or service development, quality control or research purposes of us and our contractors and service providers, and

(f) handle any enquiries or complaints relevant to our financial products or services or your investment.

We may disclose your personal information to others if we are required to, such as where we are required to by—

(a) Australian Government regulators and entities such as the Australian Securities and Investments Commission, the Australian Tax Office, and the Australian Transaction Reports and Analysis Centre

(b) the Financial Ombudsman Service (FOS)

(c) court order (including in Family Law matters), or

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

It may be necessary to release information or provide access to external service providers, such as—

(a) any organisations involved in the provision of, management or administration of our products or services (such as custodians, registries, administrators, mail houses and information technology providers)

(b) auditors, consultants and other professional advisors (including accountants and lawyers)

(c) when required or permitted under law or in connection with legal proceedings, or

(d) authorities investigating (or who could potentially investigate) alleged fraudulent or suspicious transactions in relation to an investment or account.

We will not sell your personal information nor will we provide it to third parties unrelated to the management of your investment or the provision of our financial products or services to you.

Direct marketing

We may also send you direct marketing communications and information about any other products or services offered by us that we expect may be of interest to you. These communications may be sent in various forms, including mail, fax and email. At any time you may opt-out of receiving marketing communications from us by contacting us (see contact details below).

Please note that, if we are currently providing you with services or products, we will still need to send you essential information about your account, the relevant services or products and other information required by law.

How you can access and correct your personal information held by us

You may request access to any of your personal information held by us. Generally, if the personal information held by us about you is incorrect, then we will correct it at your request.

Your right to access is subject to some exceptions allowed by law. We will notify you of the basis for any denial of access to your personal information.

Please contact our Privacy Officer using the below details to request access to any of your personal information held by us.

How can you complain about a breach of privacy?

If you have a complaint about a breach of this Privacy Policy including the manner in which we have collected, held, used, disclosed, kept, or given people access to your personal information, then you may make a complaint to us using the contact details set out below. You will need to provide us with sufficient details regarding your complaint and any supporting evidence.

Your complaint will be referred to our Privacy Officer who will investigate the issue and determine the steps we will take to resolve your complaint. We may ask you to provide additional information.

We will notify you in writing of our determination, generally within 30 days. If you are not satisfied with our determination or you do not receive a response within 30 days, then you can contact us to discuss

your concerns and you can refer the complaint to the Office of the Australian Information Commissioner www.oaic.gov.au.

Accuracy, currency, and completeness of information

We will endeavour to ensure your personal information is kept accurate, complete, up to date and relevant. Please let us know if any of your details change. If you feel your personal information is not accurate, complete or up to date, then please notify us and we will take reasonable steps to ensure it is corrected. You can contact us using the details listed below.

We will consider if the information requires amendment. If we do not agree that there are grounds for amendment then we will add a note to the personal information stating that you disagree with it.

Are we likely to disclose your personal information to overseas recipients?

We will not disclose your personal information to overseas recipients, unless required to by law.

Request a copy of this Privacy Policy and further information

A copy of our current Privacy Policy is available from us free of charge from our website, www.winim.com.au. You can also request a copy of the Privacy Policy to be sent to you—

(a) by email, by emailing your request to privacy@winim.com.au.

(b) by post, by calling 02 8021 7667 (+61 2 8021 7667 for international callers), or by writing to us.

Our postal address is:

Attn: Privacy Officer
WINIM Funds Management Pty Limited
Suite 106, 40 Yeo Street
Neutral Bay NSW 2089
Australia

If you would like a copy of this Privacy Policy in a particular form (for example, on audio disc), then please contact us and we will accommodate any reasonable request.

If you have any further questions relating to this Privacy Policy, or concerns about the way in which we have handled your personal information, then please contact our Privacy Officer.

Schedule 3—Privacy statement

In applying to invest, you are providing WINIM Funds Management Pty Limited (WFM) with certain personal details (your name, address etc). WFM uses this information to establish and manage that investment for you.

Under the *Privacy Act 1988* (Cth) you can access personal information about you held by us, except in limited circumstances. Please let WFM know if you think the information is inaccurate, incomplete or out of date. You can also tell WFM at any time not to pass on your personal information by advising it in writing.

If you do not provide your contact details and other information, then WFM may not be able to process your application to invest.

Under various laws and regulatory requirements, WFM may have to pass-on certain information to other organisations, such as the Australian Tax Office or the Australian Transaction Reports and Analysis Centre (AUSTRAC).

By applying to invest, you give WFM permission to pass information it holds about you to other companies which are involved in helping WFM administer the Fund, or where they require it for the purposes of compliance with AML/CTF law. WFM may also use your information to provide you with details of future investment offers made by the WFM.

A copy of our Privacy Policy and the Australian Privacy Principles are available free of charge on our website or by contacting us.

Schedule 4—Summary of the Australian Privacy Principles

This summary was published by the OAIC and is current as at 12 March 2014 and can be accessed on the OAIC's website, which is http://www.oaic.gov.au/.

Australian Privacy Principle 1—Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

Australian Privacy Principle 2—Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Australian Privacy Principle 3—Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

Australian Privacy Principle 4—Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

Australian Privacy Principle 5—Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

Australian Privacy Principle 6—Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

Australian Privacy Principle 7—Direct Marketing

An organisation may only use or disclose personal information for Direct Marketing purposes if certain conditions are met.

Australian Privacy Principle 8—Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

Australian Privacy Principle 9—Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Australian Privacy Principle 10—Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

Australian Privacy Principle 11—Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Australian Privacy Principle 12—Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

Australian Privacy Principle 13—Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

Schedule 5—Permitted General Situations

Item	Item applies to	Condition(s)
1	(a) Personal Information, or (b) A Government Related Identifier.	(a) It is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and (b) WFM reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	(a) Personal Information, or (b) A Government Related Identifier.	(a) WFM has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to WFM's functions or activities has been, is being or may be engaged in, and (b) WFM reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	Personal Information	(a) WFM reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and (b) the collection, use or disclosure complies with the rules made by the Commissioner for this purpose.
4	Personal Information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
5	Personal Information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.