

REI SUPERANNUATION FUND

PRIVACY PLAN

A Document prepared for and published by:

Rei Superannuation Fund Pty Ltd (ABN 68 056 044 770)

CONTENTS

	<u>Page</u>
1. Executive Summary.....	4
1.1 Plan for REISFP/L	
1.2 Development of the Plan	
1.3 Structure of the Plan	
2. Outline of the Fund.....	4
2.1 Structure	
2.2 Administration of the Fund	
2.3 REISFP/L Administration Agreement	
2.4 Investment of Funds	
2.5 Secretariat Services	
2.6 Scope of Personal Records	
2.7 Privacy Officer appointed	
3. Personal Information- Member Records	5
3.1 Maintenance of Member Information	
3.2 Type of Information Held	
4. Personal Information- Staff Records.....	6
4.1 Maintenance of Staff Records	
4.2 Records Produced by MERCER	
4.3 Records Held by Fund Secretary	
4.4 Workers Compensation	
5. Public Interest Determinations.....	6
6. Codes of Practice.....	6
7. NPP1 - Collection	8
7.1 Purpose of Collection of Member Information	
7.2 New Records	
7.3 New Information in Respect of Members	
7.4 Failure to Consent/Provide Information	
7.5 NPP1-Satisfied	
7.6 Collection of TFNs	
8. NPP2-Use and Disclosure.....	10
8.1 Disclosure to Service Providers	
8.2 Collection from Members	
8.3 Primary v Secondary Purposes	
8.4 Reasonably Expected Use or Disclosure	
8.5 Disclosure and Automatic Transfer	
8.6 Disclosure to Government Agencies	
8.7 NPP2-Satisfied	
9. NPP3-Data Quality.....	13
9.1 Quality of Collection	
9.2 Member Updates	
9.3 Accuracy/NPP3-Satisfied	
10. NPP4 – Data Security.....	14
10.1 Security Against Misuse and Loss	
10.2 Security Against Unauthorised Access	
10.3 Other Disclosure Situations	
10.4 NPP 4-Satisfied	
11. NPP5 – Openess.....	17
12. NPP6 - Access and Correction.....	17

- 13. NPPs7&8-Identifiers and Anonymity.....18
- 14. NPP9-Transborder Data Flows.....18

- 15. NPP10-Sensitive Information.....18
 - 15.1 Classes of Sensitive Information
 - 15.2 Health Information
 - 15.3 Exemption
 - 15.4 Form Consents
 - 15.5 Public Health Information
 - 15.6 Tax File Numbers
 - 15.7 NPP10-Satisfied

- 16.Principles in Respect of the Trustee’s Directors.....20
 - 16.1 Collection of Personnel Information
 - 16.2 Monitoring of E-mails and Internet Browsing
 - 16.3 Security
 - 16.4 Confidentiality Deeds
 - 16.5 Openess
 - 16.6 Quality of Information & Access and Correction
 - 16.7 Use and Disclosure

- 17.Training and Education.....21
 - 17.1 Present Knowledge of Privacy
 - 17.2 Training
 - 17.3 Interactive Education
 - 17.4 Training Schedule

- 18. Compliance Monitoring and Auditing.....21
 - 18.1 Policies and Procedures
 - 18.2 Audit Program
 - 18.3 Risk Management
 - 18.4 Audit trails -Computer Systems
 - 18.5 Low Level of Risk
 - 18.6 Review of Plan

REISF Privacy Plan (the Plan)

1. Executive Summary

1.1 Plan for REISFP/L

This Plan is prepared in accordance with The Privacy Amendment (Private Sector) Act 2000 (Cth) (**the Privacy Act**) an Act which amends the Privacy Act 1988 (Cth). It sets out how the trustee of the Rei Superannuation Fund [Rei Superannuation Fund Pty Ltd (**REISFP/L or simply, the Trustee**)] seeks to comply with the requirements of the Privacy Act.

1.2 Development of the Plan

REISFP/L has developed this Plan in order to provide a document suitable for disclosure to members and beneficiaries and in controlled circumstances and if so required by law, for more general distribution. It is a working document in that it can be altered from time to time at REISFP/L's discretion.

1.3 Structure of the Plan

The Plan is structured in the following way:

- (a) a description is given of the REI Superannuation Fund (**the Fund**) and the personal information covered by the Plan in points 2 to 4;
- (b) Public Interest Determinations and Codes of Practice are dealt with in points 5 and 6 ;
- (c) points 7 to 15 deal separately with each of the National Privacy Principles (**NPPs**) of the Privacy Act in respect of member information. A plain English summary of the NPPs, issued by the Federal Privacy Commissioner, is given at the beginning of each point;
- (d) the NPPs in respect of the Trustee's directors are addressed in point 16;
- (e) points 17 and 18 deal with training and education, compliance monitoring and review of the Plan.

2. Outline of The Fund

2.1 Structure

REISFP/L is the Trustee of an accumulation style superannuation fund that is known under the Superannuation Industry (Supervision) Act 1993 as a standard employer sponsored superannuation fund.

The Fund offers member investment choice from a limited array of Trustee approved choices and has an predominantly member elected board of directors-an approach specifically approved by the Regulator of superannuation and being a matter of difference, to the Trustee's best knowledge, to all other superannuation funds like the Fund.

2.2 Administration of the Fund

Planning for privacy compliance is complicated by the fact that, although REISFP/L is the responsible body under the Privacy Act, most of the operational functions associated with the administration of superannuation for members are actually carried out by the fund administrator, William M. Mercer Pty Limited (**MERCER**). MERCER is itself subject to the Privacy Act and as a result also has available its own 'Plan' that has application to both its clients and its business as an administrator of numerous superannuation funds but also to the extent that it acts as an agent for

REISFP/L, its activities have to comply with the Privacy Act.

2.3 REISFP/L Administration Agreement

In practice, having decided how personal information held on its behalf by MERCER is to be handled, REISFP/L will seek to ensure compliance through the terms of the REISFP/L Administration Agreement with MERCER. The Administration Agreement requires MERCER to maintain member data as necessary to administer the Fund, with a condition that MERCER complies with relevant legislation, specifically including the Privacy Act. The Administration Agreement also requires MERCER to comply with this Plan.

2.4 Investment of Funds

Investment of funds is, in most circumstances, undertaken on behalf of REISFP/L by a private sector investment manager, who is also subject to the Privacy Act.

The investment manager is the consulting and research house Intech [Intech Fiduciaries Limited (ABN 54 071 808 501)-INTECH].

Some relatively minor direct investments are carried out by REISFP/L most notably into investment bonds for the purposes of accessing for members, a 'Super Members Home Loans' facility and a 'Super Members Business Loans' facility.

2.5 Secretariat Services

A company, Superannuation Secretariat Services Pty Limited (ABN 68 056 044 770)(SSS) provides the Fund secretary and secretariat services to the Trustee, for the Fund. SSS maintains and handles personal information in relation to insurance claims, complaints and objections and also in respect of the Trustee's directors.

The written agreement between the Trustee and SSS requires SSS to maintain and use personal information in respect of members and beneficiaries provided to it by MERCER and information provided by Trustee directors in a manner that does not contravene the Privacy Act.

2.6 Scope of Personal Records

Records are maintained both on members of the Fund and on the Trustee's directors.

2.7 Privacy Officer appointed

Mr Phillip Roberts, a gentleman well acquainted with the Fund over his approximately 15 years of exposure to it as consultant and Fund Secretary (on behalf of the company, SSS) has agreed to act as the privacy officer for the Fund. He was appointed to that position on 7 December 2001 and can be contacted at the address listed for the Complaints Officer at point 11 of this Plan.

3. Personal Information - Member Records

3.1 Maintenance of Member Information

Information about each of the around 25,000 members is held by MERCER. One main computer database system known as SUPERB stores the bulk of the members' information, while a minor system holds some records for the purposes of accounting and ancillary services to the Fund. SSS and the Trustee's directors hold some paper records, mainly on members' inquiries, complaints, objections and disputes, but otherwise have access to most of the computer records maintained by MERCER on an as needs basis.

3.2 Type of Information Held

The information held about members includes basic identifying and contact details (eg: name, address, phone no, date of birth, gender); details of their employment (eg: commencement dates); salary; relevant leave periods; applications and choice forms covering investment choices and optional insurance cover and a contributions history. In due course, a member's record will possibly include a benefits payment history, details of a termination payment or of a transfer payment to another fund. Where a member makes a claim for a total and permanent disability benefit or a salary continuance benefit or the member unfortunately becomes deceased, additional information will be held about the claim, including if applicable, medical details, beneficiary details and expert advice. The REISFP/L is required by law to invite members to quote their tax file numbers (if a member chooses not to, tax is withheld from their benefit at a higher rate than would otherwise apply).

4. Personal Information - Staff Records

4.1 Maintenance of Staff Records

REISFP/L does not employ any staff. Records of remuneration of the Trustee's directors, the independent chairperson and service providers are contained in the minutes of Trustee director meetings. That information is not a matter of public record. However, Trustee director remuneration for any particular financial year, is reported in the Trustee's annual report for that year.

4.2 Records Produced by MERCER

Reports on superannuation entitlements in respect of REISFP/L's directors are produced from the SUPERB system and sent to the Fund's secretary. Relevant records of payment are maintained in MERCER's accounting system.

4.3 Records Held by Fund Secretary

The Fund's secretary is responsible for raising invoices relating to remuneration of Trustee directors and the chairperson. Relevant records of payment are maintained in MERCER'S accounting system.

4.4 Workers Compensation

In the event of a workers compensation claim, a separate file would be held by the Fund secretary, with a copy of the file kept by the insurer.

5. Public Interest Determinations

Part VI of the Privacy Act contains special provisions relating to public interest determinations. REISFP/L does not consider that there is important information for disclosure to members at present under this heading of the Plan.

6. Codes of Practice

The Privacy Act provides an ability for individualised 'Privacy Codes' to be developed by organisations where they wish to or need to depart from compliance with the NPPs. REISFP/L has not identified any need to depart from the NPPs, and will not therefore be submitting any Codes for approval by the Federal Privacy Commissioner.

A detailed consideration of each of the NPPs and how they apply in practice in the Fund, follows on the succeeding pages of the Plan.

7. NPP1 – Collection

Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, that the person can get access to their personal information and what happens if the person does not give the information.

7.1 Purpose of Collection of Member Information

- (a) This activity of REISFP/L is for the purpose of:

The administration of superannuation and related investment and insurance for members, in accordance with the relevant legislation and the Fund's governing rules, including collection of contributions, calculation of benefits and eventually the paying of a benefit or the transfer out of an applicable sum to another suitable superannuation arrangement.

As the purpose for which REISFP/L collects personal information primarily relates to the function or activity of REISFP/L as the trustee of a superannuation fund, NPP1 is therefore satisfied. This information may be supplied to MERCER or may come to REISFP/L via MERCER. Some additional fields on MERCER's SUPERB system may as a result, be 'populated' in members soft 'Files'.

- (b) Additional information is collected when a member approaches retirement or leaves employment for any reason (including death), and needs to make decisions or decisions need to be made in respect of them about the form or ultimate receiver of their benefits.
- (c) If REISFP/L is in any doubt as to whether the use(s) it intends for information collected by it is directly related to its 'primary purpose' for collection, informed and specific written consent will be sought (see point 8).

7.2 New Records

New records are created in respect of members when they join the Fund and at subsequent times.

7.3 New Information in Respect of Members

New information can be created or added to a member's file or record. This can arise as follows:

- (a) The contributions history is regularly updated :
- (i) from returns from employers; and
 - (ii) from members voluntary contributions in respect of themselves and/or their spouses.

Also, salary and employment details are provided as necessary by employers.

- (b) A member may make a written enquiry or complaint concerning their superannuation, in which case details of the enquiry and response will be recorded both in hard and soft copy. Soft copies of the format of annual statements sent to members are also maintained. A written enquiry may develop into a complaint or formal appeal or dispute under superannuation legislation, in which case additional information will be collected and held.
- (c) A member's nomination of beneficiary form or change of beneficiary form for the purposes of giving an indication to the REISFP/L's directors of where the member would like their death benefit paid is held in paper form in MERCER files as are any change of investment choice and optional insurance cover forms applicable to the member. Details taken from these forms may be used by MERCER to populate more 'fields' on its SUPERB database in respect of the member.
- (d) If a member makes a claim for a total and permanent disability benefit or a salary continuance benefit, then additional details, including medical reports, will be obtained from the Fund's insurer and with the member's consent (obtained generally or in some circumstances specifically), possibly further information as required.

This information may be supplied to MERCER or may come to REISFP/L via MERCER. Some additional fields on MERCER's SUPERB system may as a result, be 'populated' in the members soft 'File'.

- (e) Additional information is collected when a member approaches retirement or leaves employment for any reason (including death) and needs to make decisions or decisions need to be made in respect of them about the form or ultimate receiver of their benefits.

7.4 Failure to Consent/Provide Information

Failure on the part of a member or beneficiary to provide consent or information when requested and in a reasonable time period after the request, could result in REISFP/L, MERCER and in some circumstances, the Fund's insurer being unable to view a benefit claim as payable (particularly as regards any insured component).

Also, benefit limitations or restrictions on amounts otherwise payable in future may be applied.

7.5 NPP I- Satisfied

REISFP/L is satisfied that in all of these circumstances the personal information collected is reasonably necessary and directly related to the purpose of collection, thereby satisfying NPP1.

REISFP/L does not collect any personal information by unlawful means .

The third part of NPP1 requires that collection not be intrusive. REISFP/L and MERCER do not generally collect information in circumstances where this is likely to be an issue. The only exception might be some insurance cases where the Fund secretary and MERCER administration staff are dealing with members who are seriously ill or with bereaved relatives. The Fund Secretary and MERCER employees likely to encounter such situations have been trained to approach them with sensitivity and maturity.

7.6 Collection of TFNs

Tax file numbers are collected in accordance with the strict requirements of the Tax File Number Guidelines issued by the Privacy Commissioner under the Privacy Act .

8. NPP2 – Use and Disclosure

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

8.1 Disclosure to Service Providers

Members' personal information is disclosed to a number of different service providers. For example:

- (a) mailing houses are contracted to mail out statements and other occasional correspondence to members;
- (b) REISFP/L engages an auditor to provide audit and ancillary accounting services in respect of the Fund;
- (c) solicitors, barristers and medical specialists are engaged to provide expert advice and represent REISFP/L if necessary in respect of tribunal and/or court proceedings;
- (d) computing or information technology professionals are contracted to assist MERCER with the provision of information technology services;
- (e) should REISFP/L enter into a strategic alliance with an organisation offering financial planning services, disclosure of members' personal information for the purposes of provision of those services may be involved; and
- (f) of course disclosure to MERCER for the purposes of Fund administration, happens routinely.

8.2 Collection from Members

Where collection is directly from the member, this brings with it the obligation under NPP 2 to only use or disclose information for the purpose for which it was collected unless a situation of consent exists. REISFP/L seeks to satisfy this requirement in a number of ways:

- (a) All standard forms used to collect personal information will via an included 'notice' make clear the purpose of the form, a member's rights under the Privacy Act and the name and address of the collecting organisation, (ie most usually, MERCER).
- (b) Information collected in disability or death benefit claim forms and applications for cover for additional insurance benefit is often disclosed to a third party such as a medical expert or external lawyer (in cases of dispute). Standard forms used for these purposes including the member's membership application form will include a specific and detailed privacy notice, together with advice of intended third parties to whom such information would normally be disclosed.
- (c) The privacy notices discussed in paragraphs (a) and (b) will be included on forms either by sticker as an interim measure or integrally as the forms are reviewed as reprinting is required. The privacy notices will be reviewed at reprinting time and any changes will be included in reprinted forms.
- (d) A further explanation in the way of a short summary of the manner in which personal information is handled will be set out in a privacy statement included in the annual Trustee report publication which is mailed to members with their annual benefit statements.
- (e) The Fund's website able to be accessed at www.reisuper.com.au, contains a suitable privacy

statement and links to this Plan in that respect.

- (f) Members or their representatives making telephone enquiries are not presently monitored but if that policy alters, the caller will be informed by a recorded message that their call may be monitored.

8.3 Primary v Secondary Purposes

Disclosure to service providers is usually only made where the disclosure is 'directly related' to the purpose for which the information was collected (or generated)-this is the 'primary purpose' area.

While this is correct in relation to most services, there are some service areas, such as the briefing of legal counsel, or of medical experts where this cannot be assumed to be the case. This brings into view the issue of 'secondary purpose'. Secondary purposes are explained further at points 8.4 -8.6 of the Plan.

8.4 Reasonably Expected Use or Disclosure

In some cases uses or disclosures to service providers may be ones of which the members are 'reasonably likely to be aware'. To assist members' further understanding of the likely secondary uses or disclosures of their personal information, REISFP/L includes in its 'notification' statement to members on member application forms, requests for additional insurance cover and for investment choice changes and in annually issued Trustee reports, a clear explanation that REISFP/L may disclose personal information to certain third parties. This will ensure that members are reasonably likely to be aware of any such disclosures for 'secondary purposes'.

Additionally though, REISFP/L will invite all major users or receivers of disclosure of 'secondary' information in respect of a member to agree to solemn undertakings of confidentiality in respect of that information. Whilst not foolproof, at least this is designed to bring home the importance and sensitivity of the information to that user or receiver.

8.5 Disclosure and Automatic Transfer

- (a) REISFP/L relies on Section 243 of the *Superannuation Industry (Supervision) Act 1993* and Regulation 10.01 of the Regulations to that Act for authority to take transfer action to the last notified Eligible Rollover Fund in some circumstances without the express consent of the member involved. Members receive notice of the intention to transfer their balances in this manner by a direct mailing to their last known address, and by means of an item in the Trustee's Annual Report.
- (b) The disclosure of personal information to the Colonial SuperTrace ERF, being the Trustee's last chosen Eligible Rollover Fund and as stated in paragraph (a), authorised by law, complies with NPP 2.

8.6 Disclosure to Government Agencies

(a) Agencies to Whom Information is Disclosed

A number of government agencies are authorised by law to access the records of superannuation funds. These include the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), Australian Taxation Office (ATO), the Child Support Agency, Centrelink, the Department of Veterans Affairs and the state or territory's Office of the Protective Commissioner and the offices of the Receiver for Unclaimed Monies. Federal and state police may on occasion wish to obtain information, and warrants and court orders (subpoenas) are occasionally served (in most family law cases the member concerned will typically request the relevant information). Other state or territory agencies may on occasion request information from the REISFP/L or MERCER, but these requests would not generally include member information at the individual account level.

(b) Delegation to MERCER to Disclose Information

REISFP/L has delegated the discretion to deal with these requests to MERCER. MERCER policy is to satisfy itself as to the legal authority for any request from a government agency for member information. MERCER is required to document the authority for any request and report quarterly to REISFP/L.

(c) Legal Authority Required

In some cases, such as APRA, ASIC and the ATO, the legal requirement extends to routine reporting, and computer reports are generated to meet the obligation. Centrelink also cite the relevant section of the *Social Security Act* in support of their requests, which are usually for 'bulk' information for use in matching programs. In other ad hoc cases, such as with police investigations and court proceedings, MERCER require production of an appropriate order or letter of authority and legal advice may become necessary.

8.7 NPP 2-Satisfied

REISFP/L is confident these procedures satisfy NPP 2.

9.NPP3 -Data Quality

An organisation must take reasonable steps to make sure that the personal information that it collects,uses or discloses is accurate,complete and up-to-date.

9.1 Quality of Collection

REISFP/L's directors acknowledge and those directors believe MERCER also acknowledges that quality control is one of the biggest challenges involved in managing large volumes of personal information.

In particular, the risk of incorrectly allocating information can lead to records being inaccurate or incomplete, and to the existence of duplicate records. The use of a unique member number to link related entries or items both help to reduce this risk. Employers are encouraged to use the member number, but do not always do so, and some records have to be matched on name and other particulars. The matching 'algorithms' used by MERCER in its SUPERB system to match member records are sophisticated, but difficulties are caused when, for instance, members have used different versions of their names with different employers and/or have provided different birth dates.

9.2 Member Updates

While MERCER cannot guarantee that records will never be mismatched, it is hoped that the members themselves would notice any residual incorrect allocation or omission when they receive their annual benefit statement. Members are also invited in the Trustee's annual report and statement of benefits mailing, to inform REISFP/L via MERCER, of any changes to their personal details including addresses.

The SuperFacts facility available to members via the Fund's website also provides them with the opportunity to examine their personal details that are held on-line by MERCER. This facility enables members to advise MERCER on-line of any incorrect details, records or data which comes to their notice.

9.3 Accuracy/NPP3-Satisfied

REISFP/L considers that it takes reasonable steps to ensure that personal information is of good quality and fit for the intended purpose, both when collecting it and before use, thereby satisfying NPP3 in respect of information being accurate, complete and up to date.

Access to and correction of personal information is the subject of NPP6 and is explained further at point 12 of the Plan.

10. NPP4 – Data Security

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.

10.1 Security Against Misuse and Loss

Security against misuse is addressed via ensuring adequate training of all personnel contacting member information and having detailed controls and protection mechanisms in the computer systems operated by MERCER.

Security against loss is addressed through regular back-up of all computer systems and off-site storage of the backed-up data.

In circumstances where information is no longer *needed for any purpose* by REISFP/L such as after a member leaves the Fund and all their benefits have been paid or transferred out of the Fund, affected information will be destroyed as security documentation. It should be noted here that the phrase 'needed for any purpose' includes the possible need to retain information to meet a requirement of the law.

10.2 Security Against Unauthorised Access

REISFP/L has identified the need to take security precautions against unauthorised access (and any consequent unauthorised use, modification and disclosure) in order to cover four different types of risk as discussed below.

(a) Access by employees

- (i) There is a risk of access by employees to information they are not authorised to see, or for purposes they are not authorised to undertake. This risk is addressed through access controls in the computer systems. MERCER has implemented a 'single sign-on' facility whereby an individual staff member's position carries with it a range of access authorisations controlled by the use of a single log-on id and password. This is used to restrict access and the ability to make changes to records in the member databases .
- (ii) REISFP/L has identified health information on medical statements as information which should only be accessible to those employees who need it to perform their tasks. MERCER has a policy of restricted access in respect of this information to State Manager, Fund Manager level and other employees only with the written approval of either of those.
- (iii) MERCER is presently reviewing Tax File Number protocols with a view to achieving strict compliance with the security requirements in the Tax File Number Guidelines issued under the Privacy Act.
- (iv) The use of password controlled access, and an automatic 'time-out' which disconnects users from operational systems after a period of inactivity, also help to reduce the risk of access by third parties (see paragraph (b)), ie inappropriate access by visitors or contractors, as well as by employees who do not have the prescribed level of authority.
- (v) Most employer access risks are addressed only partly by physical or logical security measures. Equally important is training and awareness of employees, so that they do not use their legitimate access to personal data to use or disclose it for

inappropriate and unauthorised purposes. This is dealt with in point 17 of this Plan.

(b) *Access by Third Parties*

- (i) There is a risk of access by third parties legitimately in contact with MERCER or REISFP/L to information they are not authorised to see. This risk includes inadvertent disclosure of members' personal information through careless actions of MERCER or REISFP/L.
- (ii) One example of 'inadvertent' disclosure would be if other member information being sent out by post appeared in the window of envelopes adjacent to addresses (a common oversight). Stationery will be checked to ensure that this does not occur.
- (iii) Large volume bulk mailings incur the risk of mismatched printing, particularly where the letter or statement extends beyond one page (as some of the member mailings do). However, there have been no reported instances in recent years of incorrect mailing by MERCER on behalf of REISFP/L. The contracts with the mailing houses require them to provide samples of each mail-out for checking by MERCER, and both MERCER and the contractors have a range of quality control measures in place which should minimise the risk of incorrect mailout.
- (iv) Information about a member can be contained in a list or table form, which could result in information about multiple members being filed on each member's file. MERCER has addressed this issue in relation to incoming information and will ensure that the only member information on a member's records is information which relates to *that* member.
- (v) Training of employees will help reduce the risks of access to third parties. The training will include reference to risks which while not currently applicable, might arise in future, such as:
 - insecure disposal of member records; and
 - inappropriate use of 'real' examples in promotional material or on the website.
- (vi) Information provided to Trustee directors needs to be carefully considered should it be handled by a third party, that no contravention of the Privacy Act occurs.

(c) *Remote Access by Third Parties (Hacking)*

There is a risk of remote unauthorised access, effectively what is known as 'hacking' into the MERCER computer systems. MERCER has assured REISFP/L that it has appropriate industry standard IT systems controls in place to guard against this risk, including 'firewalls' between the public access website and the internal network and databases.

(d) *Third Party Access by Deception or Impersonation*

- (i) There is a risk of deliberate deception or impersonation to obtain personal information by a person with no authority to see such information. One of the most common examples would be an estranged spouse seeking information about an ex-partner's financial circumstances. Federal legislation will in any case require disclosure of certain information from a date yet to be established but in 2002, but there are a range of other possibilities, involving for example private investigators or journalists.
- (ii) Privacy principles do not prescribe a particular level of evidence of identity. *Federal Privacy Guidelines* suggest organisations apply risk management principles to address this potential problem. REISFP/L needs to ensure that a good level of customer service is provided while at the same time guarding *sufficiently* against unauthorised access by persons either impersonating a member or falsely claiming to be acting on their behalf. Setting an appropriate balance in this respect is always difficult, and it is impossible to guarantee that information will never be disclosed inappropriately.
- (iii) MERCER is permitted by REISFP/L to rely on a member's signature in written dealings, as long as there is no reason to doubt that it is genuine. When dealing with members in person (whether by phone or face to face) the practice of MERCER (and REISFP/L's directors where necessary) is to require at least two pieces of personal information to be quoted, typically member number and date of birth as well as name. If the staff member dealing with an oral enquiry is in any doubt as to the bona fides of the inquirer, they are instructed to request further details which are not likely to be widely known, such as date of commencement in employment.
- (iv) The problem with relying on this evidence of identity information (particularly where there is no human interaction) is that all of the items typically requested and accepted are quite likely to be known to a disgruntled spouse or partner. The same is true of another item used by many financial institutions - mother's maiden name.

(e) *Disaster Recovery*

MERCER has in place a disaster recovery plan which relates to its business. That plan is being considered by MERCER as to any implications for it under MERCER's Privacy Plan (a separate document to this).

10.3 Other Disclosure Situations

Point 8 of this Plan specifically covers the many other situations where disclosure may be required by legislation or be necessary in order to comply with the requirements of the law generally.

10.4 NPP4-Satisfied

REISFP/L believes that the information contained in this point 10 of the Plan shows that it is deeply serious about information security. The Trustee's directors are of the view that the Trustee satisfies NPP4.

11.NPP 5- Openess

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

REISFP/L addresses this NPP via disclosure of information handling practices in the Trustee's Annual Report and via this Plan itself which is a document available to anyone who asks.

If the reader of this Plan would like further information on how REISFP/L or MERCER handles personal information, or if you are a member or other beneficiary of a benefit payable by the Fund and you wish to make a complaint about a possible breach of privacy, please write to the following address; Complaints Officer, Rei Super, Locked Bag 479, Adelaide SA 5001. Should the matter involve MERCER specifically, the Complaints Officer will take the matter up with MERCER on your behalf.

If you are unsatisfied with the resolution of any matter of privacy and wish to complain, you can refer the matter to the Privacy Commissioner by telephoning 1300 363 992.

The Trustee's directors believe that the information contained in the Plan and the open nature of REISFP/L's information handling practices, means that REISFP/L clearly satisfies NPP5.

12. NPP 6-Access and Correction

Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.

Under this NPP you have the right to know what information the Trustee and any contracted service provider holds and you are entitled to view this information to ensure it is accurate and correct. As this information is often sensitive, complex and kept in different situations, to obtain this information or at the Trustee's discretion, in order to gain personal access to the information held, you are requested to write to the address for complaints referred to under point 11 of the Plan requesting MERCER, on behalf of REISFP/L, to forward to you, your personal details or to grant access. Service providers other than MERCER who hold your information will likely need to be corresponded with by the Trustee or the Complaints Officer on a case by case basis.

You must understand that providing information to you in an electronic form may not be secure.

There are certain circumstances in which access to personal information held will be denied or restricted.

The Trustee has a right under the Privacy Act to charge a reasonable fee for access to information but not for the mere request of access. Requests for access will be dealt with as soon as possible but in any case, within 30 days of receipt of the request.

The Trustee's director's believe that REISFP/L's practices and procedures as covered under this point of the Plan, satisfy NPP6.

13. NPP's 7&8-Identifiers and Anonymity

Generally speaking,an organisation must not adopt,use or disclose,an identifier that has been assigned by a Commonwealth government 'agency'.(NPP 7.)

Neither REISFP/L nor MERCER use identifiers of any type which may have been assigned by a Commonwealth government 'agency'.

An individual's name or Australian Business Number (ABN) is not classed as an 'identifier' under the NPPs. Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do so.(NPP 8.)

Where it is not illegal and it is practicable to do so,REISFP/L will and the Trustee's directors believe MERCER will, allow members , beneficiaries and employers to interact anonymously in carrying out the Fund transactions available to them.

14. NPP 9-Transborder Data Flows

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

REISFP/L and MERCER will only ever transfer your personal information to a recipient in a foreign country where you have provided your specific request (consent) to do so.Any information transferred will be done on a secure basis from Australia.You should however be aware that foreign country recipients do not necessarily have the same or even similar security or privacy requirements as that required in Australia.

The Trustee's directors are sure that REISFP/L's procedures and processes as covered under this point of the Plan, satisfy NPP9.

15. NPP10 - Sensitive Information

An organisation must not collect sensitive information unless the individual has consented,it is required by law or in other special specified circumstances,for example,relating to health services provision and individual or public health and safety.

15.1 Classes of Sensitive Information

Particular classes of'sensitive' information are subject to additional constraints on disclosure.

15.2 Health Information

One class of information which is held by MERCER on REISFP/L's behalf is health information (for some members). Health information contained in medical reports associated with claims for a total and permanent disability or salary continuance benefit is disclosed to one or more of REISFP/L's medical consultants and in some cases, external lawyers when a decision of REISFP/L is subject to objection,complaint or court action.

15.3 Exemption

REISFP/L considers that these disclosures would fall within the 'exemption' provided in NPP 2.1 (b) if members concerned give their express consent to referrals where necessary when they make a claim. It is REISFP/L's policy to request specific and informed written consent to disclosure both on member application forms for additional insurance cover and when a claim is made.

15.4 Form Consents

Forms will be amended to include a consent requirement so that the disclosure of a member's information complies with NPP10, particularly as the exemption may not cover all situations.

15.5 Public Health Information

Certain States and Territories of Australia have legislation in force which may require REISFP/L to collect and use information that impliedly relates to the sexual preference of some members, including requiring REISFP/L and MERCER to exchange such member information. Whether such requirements fall within any exemptions under the Privacy Act are not known but in any case, fresh member consent would usually be sought before any such disclosure is undertaken.

If collection and provision of sensitive information is required of REISFP/L to facilitate the gathering of research or statistics relevant to public health or safety or management then the Trustee will firstly attempt to do so with de-identified data and only if that fails, with individual member consent or in accordance with published guidelines. The National Health and Medical Research Council (of Australia) has published substantial guidelines under section 95A of the Privacy Act for release of certain of this type of information and the Trustee acknowledges that.

15.6 Tax File Numbers

All superannuation funds are required by law to hold members' tax file numbers (TFNs) where members have provided them, which members need to do to avoid having tax deducted at the highest marginal rate. Although TFNs are not 'sensitive' information for the purposes of NPP10, the Privacy Act and taxation laws between them strictly limit the disclosure of TFNs, including restrictions on internal access on a need to know basis. MERCER'S SUPERB system and reporting processes have generally been designed to ensure that TFNs are only disclosed where authorised by law, for instance in regular reports to the Australian Taxation Office or for instance when a benefit is to be paid. Further steps are being considered by MERCER to ensure that there are no weak links in these controls that could lead to unauthorised access to TFNs.

15.7 NPP 10-Satisfied

REISFP/L has ensured that robust and sensible procedures and practices for handling sensitive information exist within the Fund. Therefore its directors are comfortable to report that they believe REISFP/L satisfies NPP 10.

16. Principles in Respect of the Trustee's Directors

16.1 Collection of Personnel Information

All of the information held about the Trustee's directors is directly related to, and necessary for, the normal range of human resources and payroll functions in respect of them. Basic information, including account details for payment of remuneration, is collected directly from each new director. NPPs 1 to 4 are satisfied in the collection of this information.

16.2 Monitoring of E-mails and Internet Browsing

MERCER has the capacity to monitor the e-mails and internet browsing of any users of the computer network. It does not however use this capability. If REISFP/L decided to ask MERCER to activate this capability, it would need to be satisfied that there was a problem to be rectified, and would inform affected persons accordingly, thereby complying with NPP1 (particularly that 'collection should be fair and not intrusive').

REISFP/L receives basic analysis of patterns of use of its website as a whole and the SuperFacts segment of the site in particular. Such analysis does not reveal personal information, only the internet provider and/or domain name of the user are identified.

16.3 Security

Only Fund dedicated MERCER administration staff and intellectual technology staff who work on the system have direct access to the SUPERB system in respect of the Fund, and any paper personnel files are kept locked in a cabinet under the control of the Fund secretary. These arrangements together with the matter covered under point 16.4 of this Plan appear to satisfy NPP4.

16.4 Confidentiality Deeds

In reviewing the wording of any confidentiality deeds to be signed in future by contracted service providers, REISFP/L will ensure that they cover personal information about employees and Trustee's directors as well as about members. This assists in satisfying NPP4.

16.5 Openess

REISFP/L will ensure that its directors are given general information about the type of personal information held about them and its uses. This satisfies NPP5.

16.6 Quality of Information & Access and Correction

Steps taken to maintain quality of information include collecting it as far as possible directly from the individual and by providing them with relatively easy access to information held about themselves. This satisfies NPP6.

16.7 Use and Disclosure

Uses and disclosures of personnel information are confined to personnel administration and related purposes such as training, superannuation, and reporting to Federal agencies. NPPs 7-10 will not generally be involved as such. If sensitive information must be disclosed, the principles and criteria referred to at length in point 15 of the Plan will apply also to any uses or disclosures intended under this point 16.

17. Training & Education

17.1 Present Knowledge of Privacy

All REISFP/L directors and key personnel in MERCER have already been exposed to privacy issues, to varying degrees, through their participation in the development of this Plan.

17.2 Training

All MERCER employees have been given a basic introduction to the Privacy Act and its implications for their work. Staff in key positions that involve handling of personal information have also participated in a workshop that included working through some practical examples of privacy issues.

17.3 Interactive Education

Consideration will also be given by MERCER, it is understood, to interactive education techniques such as a self completion questionnaire, which could be administered on-line.

17.4 Training Schedule

Initial training and education of MERCER and staff has been completed.

18. Compliance Monitoring and Auditing

18.1 Policies and Procedures

REISFP/L is committed to ensuring that the policies and procedures that its directors are putting in place for compliance with the Privacy Act are followed through and implemented in practice. The unusual arrangement for entities other than likely superannuation funds, where most of the Trustee's handling of personal information is carried out by another entity (MERCER), makes it all the more important that there is effective compliance monitoring and auditing.

18.2 Audit Program

A suitably qualified and APRA approved auditor provides external audit services to the Fund. REISFP/L will consider inviting the auditor to assist in the preparation of an audit program to periodically test that the provisions of this Privacy Plan are being implemented, and that REISFP/L and MERCER, on behalf of REISFP/L, are complying with the NPPs. If REISFP/L decides to add this area to the duties of the auditor, the auditor will report to REISFP/L and its Compliance and Audit Committee which includes as its participants, external, independent and professionally qualified persons, experienced in superannuation matters.

18.3 Risk Management

Any audit program implemented in respect of this Plan and Privacy Act principles in general will apply risk management principles to identify the areas of personal information handling where there is the greatest risk of breaches of the NPPs and serious potential consequences.

18.4 Audit trails - Computer Systems

One important tool for compliance monitoring and auditing will be the use of audit trails on the MERCER computer systems. Like most such systems, the MERCER systems have the capability to record transactions to a high level of detail if required. But there is a trade-off in terms of processing time and storage, both of which have a financial and an opportunity cost.

18.5 Low Level of Risk

Given the relatively low level of risk, and of harm that could result from unauthorised access, the Trustee's directors accept that it is not necessary to record the detail of each employee's sessions logged on to the member databases. On the other hand, the directors consider that it would be desirable for MERCER to keep a record of which employees access sensitive health information in member files (soft or hard), and when. The system currently identifies a staff member who makes changes to sensitive information and MERCER may consider reviewing its system to see whether identification could be extended to staff members who merely access the information.

18.6 Review of Plan

The Plan will be monitored continuously and any changes needed to reflect new systems or processes, legislative amendments or advice or guidelines issued by the Privacy Commissioner will be made as soon as practicable.

In addition, REISFP/L will undertake a formal review of the Plan after two years (between July and December 2003).

THIS PAGE AND THE FOLLOWING PAGES ARE INTENTIONALLY LEFT BLANK SO THAT THE READER MAY MAKE APPROPRIATE NOTES.

