Privacy Policy

	Date Actual or Expected	Responsible
Last Reviewed	24 February 2020	Audit and Compliance Committee
Last Approved	24 February 2020	Audit and Compliance Committee
To be reviewed by	22 February 2021	Audit and Compliance Committee
To be approved by	22 February 2021	Audit and Compliance Committee

Table of Contents

1. Purpose

Christian Super ABN 66 628 776 348 ("the Fund") has adopted this Privacy Policy to ensure that it handles private information about individuals responsibly and in accordance with legislation. It is important that individuals dealing with the Trustee are confident that the Trustee respects the security of their personal information and does not interfere with their privacy when handling this information. The Trustee abides by the Australian Privacy Principles ("APPs") under the *Privacy Act 1988* (Cth).

The primary group of individuals for whom the Trustee collects information is for members, and this policy is accordingly framed in respect of members. While not explicitly covered by this policy, the Trustee will take all reasonable steps to handle private information collected on behalf of non-member individuals (including employees, employers and potential members) in a manner consistent with the provisions of this policy and commensurate with the nature of data collected, and commits to abide by the APPs and all other legislative and regulatory obligations in the handling of this information.

2. Personal and Sensitive Information

2.1. Personal Information

The Trustee holds and uses personal information about each Fund member. Typically this may include a member's:

- names,
- address,
- date of birth,
- gender,
- marital status
- occupation,
- salary,
- email address,
- contact details, and
- any other required information.

This information is needed to maintain the Fund's records in a format that identifies the member. These records are essential to the proper management of the Fund and to enable the Trustee to provide members with superannuation and insurance benefits, and to address specific member enquiries.

2.2. Sensitive Information

The Trustee might also collect sensitive information about a member, including health information, to enable it to obtain various insurance products on behalf of the member from the Fund's insurers, or to process a member's insurance claim. Information about a member's potential beneficiaries is also held by the Fund.

2.3. Tax File Number Information

The Trustee also collects a member's Tax File Number (TFN) in order to administer superannuation benefits. Members are not legally obliged to quote their TFN. However, there may be financial consequences for members who choose not to quote their TFN. TFN information is handled in accordance with the *Tax File Number Guidelines 2011*, issued under the *Privacy Act*.

3. Australian Privacy Principles

The Trustee is committed to the privacy of members and ensuring the rightful management and security of information which members have provided to the Trustee in accordance with the Australian Privacy Principles (Schedule 1 of the *Privacy Act 1988*).

3.1. APP 1: Open and transparent management of personal information

The Trustee will maintain and abide by a Privacy Policy which is regularly reviewed to ensure compliance with relevant legislation. This policy will contain information about the management of personal information by the Trustee. An abridged version of this policy will be made available to members on the Fund website, or provided in any reasonably requested medium upon request, free of charge.

3.2. APP 2: Anonymity and pseudonymity

The Trustee will not refuse to deal with individuals who do not disclose their true identity. However, this applies to general enquiries only. Enquiries relating to:

- specific account information; or
- the administering of superannuation benefits or insurance claims; or
- issues where the Fund is lawfully required to obtain identification; or
- issues where it is impracticable for the Trustee to deal with an unidentified individual

will require identity verification in order for the Trustee to deal with the individual.

3.3. APP 3: Collection of solicited personal information

The Trustee collects personal and sensitive information to the extent that it is reasonably necessary to administer superannuation benefits and insurance claims to members, or where it is legally obliged to do so. Furthermore, sensitive information is only collected with the member's consent.

The Fund usually collects personal information directly from members or from their employer. However, some personal information may be collected from other sources including doctors, insurers and government agencies. The collection of sensitive information, including health information for insurance applications or claims is directly collected from the member. Information about potential beneficiaries of a member's death benefit is collected from the member and is not used until the member's death.

If a member decides not to provide the Trustee with the information needed, or not to allow their employer to provide the Trustee with that information, then the Trustee may be limited in

providing superannuation benefits to the member. Where the information is health information, this may limit the level of insurance benefits available to the member through the Trustee. If the Trustee does not hold a member's TFN, there may be taxation implications, and the transfer of "lost" entitlements to government bodies may also be impacted.

Christian Super maintains a website accessible to the public which collects information through persistent and non-persistent cookies. This includes IP addresses and timestamps and is retained on average for 12 months. The Trustee does not collect personally identifiable information from the public section of the website unless provided. Information collected when members log-in to the secure section of the website in order to access their personal account includes the:

- date and time of visit,
- pages viewed,
- internet protocol address, and
- operating system used.

The handling of the information collected under APP 3 is covered in APP 5 to 13.

3.4. APP 4: Dealing with unsolicited personal information

All paper correspondence that the Trustee receives is immediately scanned into our database and telephone calls are automatically recorded by the Trustee or its outsourced administration service provider.

Where the Trustee has received unsolicited personal information in a communication that is not information that the Trustee could have collected under APP 3, the information will be destroyed or de-identified where it is lawful and reasonable to do so as soon as practicable.

If the unsolicited personal information is information that the Trustee could have collected under APP 3, the information will be treated as information collected under APP 3.

3.5. APP 5: Notification of the collection of personal information

The Trustee will notify individuals of the collection of personal information as soon as is practicable and will include the following details, as is reasonable, with consideration of the circumstances of the collection:

- identity and contact details of the Trustee,
- if the individual may not be aware of the collection, notification of the collection and the circumstances under which it occurred (e.g. supplied by an employer),
- if the Trustee is legally obliged to collect the personal information, notification that the collection is required,
- purpose of the collection and any consequences for the individual if the information is not collected,
- any parties to which the Trustee discloses personal information of the kind collected,
- that the Trustee's Privacy Policy contains information about how the individual may:
- access the information and seek its correction;

- complain if the Fund breaches its privacy obligations, and how complaints are handled,
- whether the Trustee is likely to disclose the personal information to overseas recipients, and if practicable, the specific countries.

3.6. APP 6: Use or disclosure of personal information

Personal information is collected and used or disclosed for the purpose of administering superannuation and insurance benefits to the members. The Trustee does not sell or rent out information. The Trustee will only use or disclose information to a third party for a secondary purpose where:

- consent is given for the use or disclosure; or
- it is reasonably expected that the Trustee would use or disclose the information for a secondary purpose, if the secondary purpose is:
    - directly related to the primary purpose, if it is sensitive information, or
    - related to the primary purpose, if it is personal information; or
- a permitted general situation exists under section 16A and 16B of the *Privacy Act 1988*; or
- the Trustee is legally obliged to use or disclose the information.

In undertaking its obligations to its members, the Trustee outsources some of its operations to other organisations. For this purpose personal or sensitive information may, as required, be transferred to or handled by:

- the Fund's administrator;
- third party providers of products and services to Fund members, including Insurance;
- Government bodies such as the Australian Taxation Office;
- the Trustee legal and other professional advisers; and
- other business support providers, including document storage, printing and collating companies.

Should a member become a member of another superannuation fund, their personal information may be transferred to that fund. Further, the employer may be provided with the member's personal information to facilitate provision of benefits in the ordinary course of their employment.

The Trustee does not ordinarily disclose personal information to overseas recipients.

3.7. APP 7: Direct marketing

The Trustee may reasonably use or disclose directly collected personal information to provide direct marketing communication to members. Where sensitive information is used, or if the Trustee has not directly collected personal information from the member, consent will be sought prior to issuing direct marketing communications.

The Trustee will ensure that members may easily opt out of direct marketing, and will comply with such requests. This may be communicated via telephone, email or post. Alternatively, members may change their "Communication Preferences" through the online Member Centre.

3.8. APP 8: Cross-border disclosure of personal information

The Trustee does not ordinarily disclose personal information to overseas recipients, and does not foresee reasonable circumstances where this may occur. However, in the event that the Trustee does send personal information overseas, the Trustee will take reasonable steps to ensure that the recipient satisfies Australian privacy obligations.

3.9. APP 9: Adoption, use or disclosure of government related identifiers

The Trustee does not adopt government related identifiers as an identifier of members. Unique member numbers are assigned to members for identification purposes.

Government related identifiers may be used to verify the identity of individuals, or to fulfil legal obligations including those of members, such as using TFNs to discharge member taxation obligations.

3.10. APP 10: Quality of personal information

The Trustee will take reasonable steps to ensure that the personal information collected, used and disclosed is accurate, up-to-date and complete, with regard to the circumstances of the collection, use or disclosure.

3.11. APP 11: Security of personal information

The Trustee protects personal information from misuse, interference or loss, and unauthorised access modification or disclosure by storing it on secure third-party Australian servers and on internal servers. Security features include, but are not limited to:

- comprehensive access control restrictions,
- industry standard firewall protection, and
- centrally managed and updated anti-virus software.

Access audit logs are kept to allow identification in the event of unauthorised access.

The Trustee will take reasonable steps to destroy or de-identify information that is no longer required. The Trustee does not ordinarily store personal or sensitive information on overseas servers.

3.12. APP 12: Access to personal information

Members can access and update their own personal information through the Online Member Centre (requires registration and login), or by contacting the Member Care Call Centre on 1300 360 907. A reasonable cost-recovery fee may apply for accessing personal information.

In some circumstances the Trustee is entitled to deny a member access to personal information. These include circumstances where such information is used in confidential trustee decisions or in a commercially sensitive decision making process, where the privacy of others may be

breached if the information was accessed or where the law requires or authorises such access to be denied. The Privacy Officer will provide written notice if access is denied.

The access and correction procedures outlined in this policy operate alongside the procedures outlined in the *Freedom of Information Act 1982*. Where there is a conflict between this policy and the FOI Act, the FOI Act shall prevail.

3.13. APP 13: Correction of Personal Information

Members are encouraged to inform the Trustee of any changes to their personal information as soon as possible, to ensure that the Fund can continually provide superannuation benefits to the member. If the information held by the Trustee is inaccurate, incomplete or not up to date a member may request the Fund to correct the information. The Trustee may request supporting documentation to evidence the requested change, and valid requests will be completed in a reasonable timeframe.

If the Trustee has any reason to refuse the request to correct the personal information, written notice will be provided, setting out the reasons for the refusal except to the extent that it would be unreasonable to do so.

4. Data Breaches

A data breach occurs when there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the Fund holds. All reasonable steps will be taken, in accordance with this policy and the controls outlined in the *IT Data and Security Framework*, to ensure that a data breach does not occur.

4.1. Data Breach Response Plan

The Fund has designed the following Data Breach Response Plan ("plan") in order to ensure that appropriate and timely action is taken to respond to the breach[i]. The plan will be carried out by the Privacy Officer, or by the Data Breach Response Team ("team") in the event of a serious breach. In determining whether to activate the team, the Privacy Officer will consider:

- The number of individuals affected by the breach;
- The likelihood of serious harm to the affected individual(s);
- The expected ease with which the breach can be contained and/or remediated; and
- The potential reputational impact of the breach.

The team will consist of the Privacy Officer and the Complaints Manager, and other staff members, directors or external advisors may be added for a particular response based on the skills or seniority required for that particular response.

Data breaches must be addressed on a case-by-case basis based on the nature of the incident and so discretion must be exercised in determining the specific response required to each breach. Nevertheless, the plan is intended to provide the infrastructure through which decisions can be made and action taken to respond to a breach in a timely manner. The plan contains four steps:

1. Identification of Potential Breach
2. Assessment of Potential Breach

3. Determination of Breach
4. Breach Response

4.1.1. Identification of Potential Breach

The first in responding to a data breach is identifying the breach. Any staff member may identify a suspected data breach. This may occur because of an action taken by the staff member that caused or uncovered the breach, or because an external party has communicated the breach. Where this occurs, the staff member must immediately notify the Privacy Officer or, if the Privacy Officer is unavailable, the Complaints Officer. The notification should:

- Be made orally in the first instance, given the potential need for immediate action to be taken to address the breach, covering:
    - The time and date the suspected breach was discovered;
    - The type of personal information involved;
    - The individual(s) affected by breach;
    - The cause of the breach (if known); and
    - The extent of the breach (if known);
- Then be made in written form with all available background information and explanatory material.

The party receiving the notification will make an initial assessment on whether a breach has or may have occurred. Where there are reasonable grounds to believe that a breach has occurred, the data breach response plan below will be followed. Where there are not such grounds, it is determined that no breach has occurred and no further action is required.

4.1.2. Assessment of Potential Breach

The second step in the process is assessing whether a data breach has actually taken place.

Where the data breach, if it is has occurred, is likely to result in serious harm to one or more individuals, the Fund must carry out a reasonable and expeditious assessment to determine whether there are reasonable grounds to believe that a breach has occurred. The Fund must take reasonable steps to complete this assessment within 30 days, though the intention in the usual course of events will be to complete the assessment in a much shorter timeframe given the potential risk of harm may often increase as time passes following the potential breach.

4.1.3. Determination of Breach

The third step in the process requires a determination to be made as to whether a breach has actually occurred following the assessment.

Where there are no reasonable grounds to believe that a breach has occurred, no further action will be taken. Where there are reasonable grounds to believe that a breach has occurred, the breach requires a response.

4.1.4. Breach Response

The fourth step in the process occurs once a determination has been made that a breach exists, and contains a further four sub-steps.

1. Containment and Assessment
2. Evaluation of Risks
3. Notification
4. Future Prevention

While these are listed as discrete steps, it is expected that they will regularly be conducted simultaneously given the potential integration between the steps.

4.1.4.1. Containment and Assessment

The first step in response to a data breach is to contain the breach. This has dual aims:

1. Reducing the scope of the breach - the number of individuals affected
2. Reducing the severity of the breach - the likely harm caused to the individuals affected

Remedial action may include human or technical controls, and may include the use of internal or external parties and may include disclosure. In order to determine the appropriate remedial actions, an assessment should be made as to the nature of the breach building on the information already provided by the notifier. The Fund maintains standing human and technical controls to contain potential data breaches in accordance with the *IT and Data Security Framework*.

Consideration will also be given at this stage as to whether the events that caused the breach, or the potential impacts of the breach, may constitute a business continuity event in accordance with the *Business Continuity Plan*.

4.1.4.2. Evaluation of Risks

The second step of the process is to evaluate the risks presented by the breach and to determine whether or not a notifiable breach has occurred. A notifiable breach occurs where:

- The breach is likely to result in serious harm to one or more individuals; and
- The Fund has not been able to prevent the likely risk of serious harm with remedial action taken in the previous step.

In determining the likelihood of serious harm, consideration will be given to:

- The nature and sensitivity of the data;
- The initial and ongoing existence of security systems protecting the data;
- The persons or kind of persons who have obtained, or could obtain, the data; and
- The nature of the potential harm that could be caused.

4.1.4.3. Notification

The third step is to identify who needs to be made aware of the breach and to notify them. Where the data breach has occurred because of the actions of an external party who also holds

the data, the Fund will generally take responsibility for completing relevant notification obligations.

4.1.4.3.1. Regulators and Agencies

Where a notifiable breach has occurred, the Fund must notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable by lodging a Notifiable Data Breach Statement ("statement") which must include:

- The identity and contact details of the Fund;
- A description of the breach and the grounds on which it is believed to have occurred;
- The kind, or kinds, of information concerned; and
- Recommendations about the steps individuals should take in response to the breach.

Where the breach is not a notifiable breach, the Fund may still determine it appropriate to notify the OAIC by having regard to the likelihood that the OAIC may receive complaints or enquiries in relation to the breach.

4.1.4.3.2. Affected Individual(s)

Where a notifiable breach has occurred, the Fund must, as soon as practicable after completing the statement:

- Notify all individuals at risk of serious harm; or
- Where not practicable because the Fund cannot reasonably identify all individuals at risk of serious harm, notify all individuals potentially affected by the breach; or
- Where this is not practicable because the Fund cannot reasonably identify all individuals potentially affected by the breach, publish a copy of the statement given to the OAIC on its website and take reasonable steps to publicise its content.

Where the breach is not a notifiable breach, the Fund may still determine it appropriate to notify the affected individual(s) by having regard to the ability of the individual to avoid or mitigate harm if notified and any impact the notification may have on the conduct of an investigation into the incident.

Where notification is to occur, careful consideration should be given to who makes the notification, and what information is provided. This should include any information included in the statement as well as details of the complaints process as outlined in the *Dispute Resolution Plan* and of how to lodge a complaint with the OAIC.

4.1.4.3.3. Internal and External Parties

Internal parties and external parties (namely service providers) should be notified of a data breach where:

- The breach arose from an action taken by that party, in part or in full;
- Actions taken in response to the breach will have an impact on that party; or
- Actions are required by that party in response to the breach.

4.1.4.4. Prevention

The prevention step focuses on identifying the root causes of the breach and protecting future recurrences of the breach. This will include fully investigating the cause of the breach and reaching the appropriate conclusions on how the breach came about.

Actions should be identified to prevent future recurrence, such as making appropriate changes to policies, procedures or systems, in particular this policy or the *IT Data and Security Framework*, and conducting training for internal or external parties.

4.2. Reporting and Documentation

All actual data breaches, or suspected breaches still under investigation, will be reported on a quarterly basis to the Audit & Compliance Committee in accordance with the *Compliance Programme* (for controls adequacy implications) as well as to the Community Engagement Committee (for stakeholder servicing implications).[ii] All investigations and findings should be fully documented and records maintained for future reference.

5. Staff Training

All employees will receive annual training on the requirements of this policy.[iii]

6. Resolution of Privacy Concerns

This policy is to be available on the Fund's website at all times, in accordance with the requirements of the *Privacy Act*.[iv] If a member is concerned about a possible interference with privacy, the member should notify the Privacy Officer in writing. Such a concern may be treated as a complaint in accordance with the *Complaints Handling Policy*, which is outlined in the *Product Disclosure Statement*. If the member's concerns are not resolved to the satisfaction of the member, the matter can be referred to the Superannuation Complaints Tribunal. If the matter is still not resolved to the satisfaction of the member, the matter can be referred to the Office of the Australian Information Commissioner.

7. Contact the Privacy Officer:

The Trustee will at all times have an appointed Privacy Officer, who shall have the responsibility as outlined through this policy. The Head of Product, Contracts & Innovation will act as the Privacy Officer. The details of the Privacy Officer must be made available on the Fund's website as follows[v]:

Name: The Privacy Officer

Address: Christian Super PO Box 3035 RHODES NSW 2138

Telephone: 1800 45 15 66

E-mail: privacy@christiansuper.com.au

8. Review

The Trustee is committed to ensuring the privacy of members and their information. The Privacy Policy will be reviewed on an annual basis by the Audit and Compliance Committee, or

more frequently if there are significant changes to legislation or regulations..[vi] This review will specifically consider the data breach response plan and whether it remains effective.

Document History

2 March 2015 Adopted by Trustee Board (Community Engagement review)

Relevant Documents

Privacy Act 1988

Tax File Number Guidelines 2011 (issued under the Privacy Act 1988)

Dispute Resolution Plan

Link Group Privacy Policy

Compliance Tasks

[i] Data Breach Response Plans

[ii] Quarterly Data Breach Reporting

[iii] Annual Privacy Training

[iv] Privacy Act Disclosure Attestation

[v] Annual Privacy Officer Website Disclosure

[vi] Annual Privacy Policy Review

Appendix A – Data Breach Response Plan

STEP 1 - IDENTIFY POTENTIAL BREACH

The Fund identifies that there are reasonable grounds to suspect that there may have been a data breach.

↓

STEP 2 - ASSESS POTENTIAL BREACH

Is the data breach, if it has occurred, likely to result in serious harm to one or more individuals?

If YES,	**If NO,**
The Fund must (*PA* s26WH(2)): • Carry out a reasonable and expeditious assessment to determine whether there are reasonable grounds to believe that a breach has occurred (*PA* s26WH(2)(a). • Take reasonable steps to complete the assessment in 30 days (*PA* s26WH(2)(b).	The Fund will endeavor to carry out an assessment as if the potential breach was a notifiable breach.

↓ ↓

STEP 3 – DETERMINE BREACH

Following the assessment, are there reasonable grounds to believe that a breach has occurred?

If YES,	**If NO,**
Respond to the breach using Step 4.	Take no further action.

↓

STEP 4 – RESPOND TO THE BREACH

STEP 4.1 – CONTAIN THE BREACH

Contain the breach, based on assessment, to reduce the scope and severity.

STEP 4.2 – EVALUATE THE RISKS

Determine likelihood of harm to individuals, including:

- The nature and sensitivity of the data;
- The initial and ongoing existence of security systems protecting the data;
- The parties who have obtained, or could obtain, the data; and
- The nature of the potential harm that could be caused.

STEP 4.3 – CONSIDER BREACH NOTIFICATION

Is the breach, after containment steps taken, likely to result in serious harm to one or more individuals?

If YES	**If NO**,
The Fund must: • Lodge a statement with the OAIC (PA s26WK). • Notify individuals at risk of serious harm (PA s26WL).	The Fund will consider whether to notify individuals or the OAIC.

STEP 4.4 – PREVENT FUTURE BREACHES

Steps are taken to identify the root cause of the breach and prevent future recurrences.