INFORMATION SECURITY POLICY

PURPOSE

The purpose of the Information Security Policy is to ensure that full and accurate records of all activities and decisions of the Long Service Leave Fund ("the Fund") are created, managed and retained or disposed of appropriately, and in accordance with relevant legislation.

SCOPE

This document applies to the Long Service Leave Board ("the Board"), the Fund Administrator and key advisors to the Fund, including third-party consultants engaged by the Board.

RECORDS AS A RESOURCE

The Fund recognises that records are a vital asset to:

- facilitate information accessibility, and enhance management and administration of the Fund;
- deliver customer services in an efficient, fair and equitable manner;
- provide evidence of actions and decisions and precedents for future decision making; and
- protect the rights and interests of the Fund, Dioceses and participating organisations, and participants of the Fund.

GENERAL PRINCIPLES

The Fund manages information in compliance with the Privacy Act 1998 (Cth) and the Australian Privacy Principles (APPs). The APPs regulate the manner in which personal information is handled throughout its lifecycle, from collection to use and disclosure, storage, accessibility and disposal.

The Fund Administrator, on behalf of the Board, is responsible for the appropriate creation and storage of records relating to their role. The Fund Administrator must comply with the correspondence and records keeping procedures in place from time to time.

RECORDS MANAGEMENT

Creation and capture

The Fund Administrator should ensure that official records are created of all decisions and actions made in the course of the management and administration of the Fund.

Storage

Current hardcopy records should be stored in designated storage areas with access restrictions. Rarely used records or records no longer in use for official purposes that are still required to be retained are maintained in a secure offsite storage facility.

ABN: 62 006 508 372 ● Suite 4, Level 5, 189 Kent Street, Sydney NSW 2000
Tel: +61 2 8267 2710 ● Fax: +61 2 8267 2727 ● www.anglican.org.au
Email: longservice@anglican.org.au

Electronic records may either be retained online (on servers) or offline (on USBs, CD Roms, magnetic disks or other removable media). Records of short-term value will be disposed of at suitable intervals by the Fund Administrator.

Access
Records must be available to all authorised Board members, Fund advisors, Diocese and participating organisations that require access to them for business purposes. No information under the stewardship of the Fund may be accessed without the appropriate authority.

The Fund will not permit access to records or disclose information where such access or disclosure would be:

- contrary to any law in force at the time, for example laws relating to defamation, breach of confidence, infringement of copyright, adoption of children; or
- a breach of a person's reasonable right to privacy.

Access is authorised as follows:

Access Status	Information	Authorised Access
Confidential/Sensitive	• LSL Database (member files, quarterly returns, leave balances, operational reports) • Payment summaries	• Fund Administrator • Diocese and participating organisations (for their organisation only) • Fund Actuary • External Auditors
High Security	• Board meeting papers and minutes • Reports from key advisors • Financial information	• Fund Administrator • Board members • Diocese and participating organisations (for their organisation only) • Key advisors (as appropriate)
Open	• Long Service Leave Canon • Fund policies and procedures, and guidelines • Annual Financial Statements	• Not limited.

Advisors and Third-Party Consultants
All records created by advisors and third-party consultants performing work on behalf of the Fund belong to the Fund. This includes the records of contract staff working on the premises as well as external service providers.

Disposal
Records that have been identified as being approved for destruction may only be destroyed once the Fund has ensured that all other requirements for retaining the records are met. Reasons for longer retention can include legal requirements, administrative need, and government directives.

The Fund must not dispose of any records where the Fund is aware of possible legal action [including legal discovery, court cases, and formal applications for access] where the records may be required as evidence.

Once all requirements for retention have been met, destruction of records should be carried out in a secure and environmentally sound way.