Lindfield Bowling & Bridge Club

Serving the Community Since 1952

DATA PRIVACY & SECURITY POLICY

Version Control

Date	Version	Author	Details
Mar 2026	Draft	Sharon Thompson	Initial policy adoption
15th July ‘26	V1.0	Sharon Thompson	After Board review

Board Approval Date: 15th july

Policy Owners: Board of Directors/Bowls Committee/Bridge Committee

DATA PRIVACY & SECURITY POLICY

Lindfield Bowling & Bridge Club

A Registered Club under the Registered Clubs Act 1976 (NSW)

1. Purpose

This Policy sets out how Lindfield Bowling & Bridge Club (the Club) collects, uses, stores, protects and disposes of personal information. It reflects the Club's commitment to handling personal information responsibly and in accordance with applicable law.

> **Privacy Act Threshold Note**
> The Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) apply to organisations with annual turnover exceeding $3 million. Regardless of legal obligation, the Club adopts these principles as best practice given the volume and sensitivity of member, payment and health data held. The Club will confirm its legal status with its adviser at each annual policy review.

2. Scope

This Policy applies to all Directors, the Club Manager, staff, volunteers, and any third party acting on behalf of the Club, in relation to personal information about:

- Current, former and prospective members
- Staff and volunteers
- Contractors and service providers
- Any other individual whose personal information the Club holds

3. What Personal Information We Collect

The Club may collect and hold the following categories of personal information:

3.1 Member and Contact Information

- Full name, date of birth, postal and email address, phone number
- Membership category, ABF number, masterpoints and game history (via Pianola)
- Emergency contact details
- Payment card details and transaction history (via Square and WooCommerce/MyAccount portal)
- Direct debit and bank account details where applicable

3.2 Staff and Volunteer Information

- Employment or engagement records, tax file number declarations, superannuation details
- Working With Children Check details where applicable
- NSW Competency Cards (Responsible Service of Alcohol)
- Bank account details for payroll

3.3 Sensitive Information

The Club may hold sensitive information (as defined by the Privacy Act) including health or medical information provided in connection with an incident or first aid. Such information is held only where necessary and with the individual's consent or as required by law.

3.4 Digital and System Data

- Login credentials and access logs for the MyAccount member portal
- IP addresses and usage data collected through the Club website
- Communications sent via the Club's email systems

4. How We Collect Personal Information

The Club collects personal information:

- Directly from the individual at the time of membership application, renewal or registration
- Via the MyAccount member portal (myaccountnsbc.com or equivalent LBBC portal)
- Via payment processing systems (Square)
- Through email, phone or written communications with the Club
- From Pianola (the Club's membership management system)
- From third parties such as ABF (Australian Bridge Federation) where members consent and Bowls New South Wales.

The Club will only collect personal information by lawful and fair means, and only where necessary for the Club's functions and activities.

5. Why We Use Personal Information

The Club uses personal information to:

- Administer membership and manage member accounts
- Process payments and manage financial transactions
- Communicate with members about Club activities, events and news
- Manage and score bridge and bowls sessions and competitions
- Comply with legal and regulatory obligations under the Registered Clubs Act 1976 (NSW), Corporations Act 2001, and applicable tax and employment law
- Manage staff and volunteer engagements
- Ensure the safety and security of persons on Club premises
- Improve Club services and systems

The Club will not use personal information for any purpose other than those described above without the individual's consent, unless required or permitted by law.

6. Disclosure of Personal Information

The Club may disclose personal information to:

- Service providers acting on the Club's behalf (e.g. Square, Pianola, SMSGlobal, web hosting providers, ABF, BridgeNSW and Bowls NSW) — subject to appropriate data processing agreements
- ABF or state bridge associations for the purpose of masterpoints registration and national membership records

- Government agencies or regulators where required by law (e.g. Liquor & Gaming NSW, SafeWork NSW, ATO)
- The Club's legal advisers, auditors or insurers in connection with their services

The Club will not sell, rent or trade personal information to any third party for commercial purposes.

Overseas Disclosure

Some Club service providers (e.g. Square, cloud hosting) may store or process data outside Australia. Where this occurs, the Club will take reasonable steps to ensure those providers handle data in a manner consistent with Australian Privacy Principles.

7. Data Security

7.1 Organisational Controls

- Access to personal information is restricted to Directors, the Bridge Club Manager, Bridge Directors, Bowls Selectors and staff on a need-to-know basis
- All persons with access to personal information are required to comply with this Policy
- Staff and volunteers handling personal data receive appropriate training
- The Club maintains a register of third-party systems holding member or payment data

7.2 Technical Controls

- All Club websites use SSL/HTTPS encryption
- Payment data is processed via PCI-DSS compliant systems (Square) and is not stored on Club systems
- Employee payroll records are maintained securely in MYOB for compliance with ATO Single Touch Payroll (STP) reporting requirements and MYOB's Superannuation Clearing House processing.
- The MyAccount member portal uses strong password policies and access controls
- Google Workspace (Drive, Sheets, Gmail) access is restricted by role and requires two-factor authentication where available
- Regular backups are maintained for all critical Club systems

7.3 Physical Controls

- Physical records containing personal information (e.g. membership forms, incident reports) are stored securely and access-controlled
- Documents containing sensitive personal information are shredded when no longer required

8. Data Retention and Disposal

The Club retains personal information only for as long as necessary for the purposes for which it was collected, or as required by law. General retention guidelines:

Category	Retention Period	Disposal Method

Member records (active)	Duration of membership + 1 years	Secure deletion / shredding
Financial records & invoices	7 years after end of financial year (ATO requirement)	Secure deletion / shredding
Incident reports	7 years	Secure deletion / shredding
Employment records	7 years after engagement ends	Secure deletion / shredding
CCTV footage (if applicable)	30 days unless subject to incident	Automatic overwrite
Website/portal access logs	12 months	Automatic deletion

9. Access and Correction

Individuals have the right to request access to personal information the Club holds about them, and to request correction of any inaccurate, out-of-date or incomplete information.

Requests should be made in writing to the Club Secretary. The Club will respond within 30 days. Access may be refused in limited circumstances permitted by law, in which case the Club will provide written reasons.

10. Data Breach Response

If a data breach occurs or is suspected, the Club will:

1. Contain the breach immediately — limit further access or disclosure
2. Assess the breach — identify what data was affected and the likely harm
3. Notify the Board — the IT Manager must notify the Chairman and Club Secretary within 24 hours
4. Notify affected individuals — where the breach is likely to cause serious harm, affected individuals will be notified promptly
5. Report to the OAIC — if the Club is covered by the Notifiable Data Breaches scheme, report to the Office of the Australian Information Commissioner within 30 days of becoming aware of an eligible breach
6. Review and remediate — document the breach, the response, and any changes to controls

Notifiable Data Breaches

Under the Privacy Act 1988 (Cth), organisations covered by the Act must report eligible data breaches (those likely to cause serious harm) to the OAIC and to affected individuals. The Club will seek legal advice promptly if a breach occurs to determine its notification obligations.

11. Cookies and Website Data

The Club's websites and member portal may use cookies and similar technologies to improve user experience and for analytics. Users can control cookie settings through their browser. The Club does not use member data for targeted advertising.

12. Complaints

Any person who believes the Club has breached this Policy or applicable privacy law may lodge a complaint with the Club Secretary in writing. The Club will investigate all complaints promptly and respond within 30 days.

If the complainant is not satisfied with the Club's response, they may contact the Office of the Australian Information Commissioner (OAIC) at oaic.gov.au or 1300 363 992.

13. Policy Review

This Policy will be reviewed annually by the Board, or earlier if there is a change in the Club's systems, operations, or applicable law. The Club will monitor the $3 million threshold and potentially seek legal advice if turnover approaches that level.

Board Approval

This Policy was adopted by the Board of Directors of Lindfield Bowling & Bridge Club at a duly convened Board meeting.

Date of Adoption: 15th July 2025

Signed (Deputy Chairman):