

MANLY EAGLES BASEBALL CLUB

Information Privacy Policy

Personal information, health information and data security • 2026 review

Our commitment

MEBC will handle personal and health information respectfully, transparently and securely. We will collect only what is reasonably needed, use it for proper Club purposes, limit access, respond to privacy concerns and dispose of information safely when it is no longer required.

Policy owner	MEBC Board
Responsible officer	Board-appointed Privacy Officer / Secretary
Applies to	Board Members, employees, coaches, managers, officials, volunteers, contractors and service providers who handle information for MEBC
Approval date	To be inserted
Next review	Two years after approval, and earlier after a serious data breach or material legal/system change
Related documents	Registration privacy notice; consent and image notice; data-breach response plan; records-retention schedule; Social Media Policy; safeguarding and complaints policies; service-provider register

Replaces: The former Information Privacy Policy referring to the Victorian Information Privacy Act 2000 and Health Records Act 2001. Those Victorian laws are not the appropriate basis for MEBC's NSW operations.

1. Purpose

This policy explains how MEBC collects, holds, uses, discloses, secures, accesses, corrects and disposes of personal information. It is designed to protect members and others while allowing the Club to administer baseball, safety, membership, communications and governance effectively.

2. Legal and policy framework

MEBC will comply with privacy, health-records, safeguarding, recordkeeping, direct-marketing and data-breach laws that apply to its activities and legal status. Because statutory coverage can depend on matters such as turnover, activities and the type of information handled, the Club adopts the following as its minimum operating standard whether or not every provision is legally mandatory:

- the Australian Privacy Principles under the Privacy Act 1988 (Cth);
- the Health Privacy Principles under the Health Records and Information Privacy Act 2002 (NSW);
- the NSW Working With Children Check verification and recordkeeping requirements; and
- privacy and security obligations accepted through governing-body systems, insurers, payment services, venue arrangements and other contracts.

Policy standard and law

This policy does not determine MEBC's legal status under a particular Act. The Privacy Officer should obtain advice when coverage, notification or health-information obligations are uncertain.

3. Scope

The policy applies to personal information handled by or on behalf of MEBC in paper, verbal, photographic, audio, video or electronic form. It applies to current and former members, players, parents/carers, volunteers, employees, contractors, officials, donors, sponsors, visitors, applicants, complainants and other contacts.

4. Definitions

Personal information

Information or an opinion about an identified person, or a person who is reasonably identifiable, whether true or recorded in material form.

Sensitive information

Includes information about health, racial or ethnic origin, political or religious beliefs, sexual orientation, criminal record and certain other protected matters.

Health information

Personal information about a person's physical or mental health, disability, injury, health service or other information treated as health information by applicable law.

Data breach

Loss, unauthorised access, disclosure, alteration or destruction of personal information, or a security compromise creating that risk.

Child / young person

A person under 18 years of age.

Service provider

A third party that stores, processes, transmits or otherwise handles information for MEBC.

5. Privacy principles

- **Accountability** — MEBC is responsible for information under its control, including information handled through volunteers and service providers.
- **Data minimisation** — collect and retain only information reasonably necessary for a stated purpose.
- **Transparency** — provide a clear notice about what is collected, why, usual disclosures and how to seek access or complain.
- **Purpose limitation** — use and disclose information for the notified purpose, a reasonably expected related purpose, with valid consent, or as authorised or required by law.
- **Need-to-know access** — access is based on role and current need, not status or curiosity.
- **Accuracy** — take reasonable steps to keep information complete, current and relevant.
- **Security** — use safeguards proportionate to sensitivity, volume, location and likely harm.
- **Respect and choice** — obtain consent where required and provide practical choices where participation does not depend on the information.
- **Safe disposal** — destroy or de-identify information when no longer required, subject to legal and operational retention needs.

6. Information MEBC may collect

Category	Examples
Membership and identity	Name, date of birth, gender or competition category where required, registration number, address, contact details and membership history.
Parent/carer and emergency	Parent/carer details, emergency contacts, pickup or supervision arrangements and relationship to the player.
Baseball administration	Team, grade, position, availability, attendance, statistics, eligibility, permits, disciplinary status and awards.
Health and safety	Allergies, medical conditions, disability or adjustment needs, injury, return-to-play restrictions, first aid and incident information.
Financial	Fees, invoices, payment status, bank transaction references, reimbursements and hardship outcome. MEBC should avoid retaining full card details.
Volunteer and workforce	Role, qualifications, training, licences, references, emergency contact, WWCC verification and other role-related screening.
Media and communications	Photographs, video, audio, testimonials, newsletter preferences, social-media interactions and image-consent choices.
Governance and integrity	Meeting records, declared interests, complaints, investigations, sanctions and safeguarding information.
Technical	Account identifiers, access logs, device or security information and website or service usage data where collected.

7. Collection and privacy notices

- Collect information fairly and, where practicable, directly from the individual or their parent/carer.
- At or before collection, provide a notice stating MEBC's identity and contact, purposes, usual recipients, any required fields and consequences of not providing them, access and complaint options, and any likely overseas handling where required.
- Do not use one broad consent to cover unrelated optional activities. Separate necessary registration information from optional marketing, member-directory and image choices.
- If information is received unexpectedly, decide promptly whether MEBC could lawfully have collected it. If not and retention is not required, securely destroy or de-identify it.
- Do not collect sensitive or health information unless reasonably necessary and supported by consent or another lawful basis.
- Record material consent and withdrawal choices in a way authorised users can reliably apply.

8. Children and young people

- Use clear, age-appropriate explanations and involve a parent/carer where required by law, safeguarding practice or the child's capacity.
- Consider the young person's views and evolving capacity, particularly for images, health information and sensitive communications.
- Collect only what is necessary for participation, safety and administration. Avoid publishing a child's full name together with detailed location, routine, school, health or contact information.
- Essential Club information must not depend on a child holding a social-media account contrary to platform rules or Australian age restrictions.
- Where a parent/carer requests access or makes a decision for a young person, consider the young person's safety, capacity, confidentiality and applicable law rather than assuming access is always unlimited.

9. Health, injury and emergency information

- Ask only for information reasonably needed to provide safe participation, emergency response, reasonable adjustment, insurance or return-to-play management.
- Tell the person who will usually receive the information—for example, the Head Coach, team manager, first-aid officer or insurer—and why.
- Provide coaches and team officials only the practical information needed for the role. A diagnosis should not be widely shared when a restriction, adjustment or emergency instruction is sufficient.
- In an emergency, information may be disclosed to paramedics, hospitals, Police, a parent/carer or another person where reasonably necessary to protect life, health or safety.
- Store incident, medical and return-to-play records separately or with stronger access controls than general team information where practicable.
- Do not publish injury or health details without authority. Public availability or player discussion does not remove the need for care.

10. Working With Children Checks and screening

- MEBC will identify roles requiring a NSW WWCC and verify each relevant worker or volunteer through the NSW Office of the Children's Guardian system.
- Verification must occur before child-related work as required and again on renewal or when otherwise directed. MEBC will keep the legally required verification record.
- Access is limited to authorised safeguarding or governance personnel. A coach or general Board Member should receive only the clearance or eligibility outcome needed for their role.
- MEBC will not request, circulate or retain police or background-check reports unless specifically authorised and necessary. The WWCC is an ongoing screening process, not a report to be shared around the Club.

- WWCC clearance does not replace child-safe recruitment, supervision, codes, reporting and risk controls.

11. Use and disclosure

MEBC may use or disclose information for the purpose notified at collection and for reasonably expected related purposes, including:

- registration, grading, competition entry, permits and player eligibility;
- team administration, scheduling, transport coordination and emergency communication;
- coaching, player development, safety, first aid, insurance and incident management;
- membership, fees, accounting, audit and governance;
- communications, awards, events and images where the applicable notice or consent allows;
- complaints, safeguarding, discipline, legal compliance and protection of people or Club assets; and
- service delivery by approved providers acting for MEBC.

MEBC may also use or disclose information with valid consent, where authorised or required by law, or where a permitted health, safety, safeguarding or enforcement basis applies.

12. Team lists, directories and group communications

- Share only the minimum contact and availability information needed for the team purpose.
- Use approved team platforms or blind-copy addressing for broad email where appropriate. Avoid exposing the full membership list.
- Do not add a person to a non-essential group, publish a directory or circulate addresses and phone numbers unless the notified process supports it.
- Members receiving team information must not reuse it for personal business, fundraising, political activity, recruitment, marketing or unrelated contact.
- Remove former participants and role-holders from groups and access promptly when the purpose ends.

13. Photographs, video and publicity

- Manage images under the Social Media Policy and the current image notice or consent process.
- Explain intended uses and usual channels. Provide a practical method to record restrictions and withdrawal requests.
- Before publication, check for sensitive information, unsafe context and people whose restrictions are recorded.
- A withdrawal will be applied to future use where reasonably practicable, but may not require removal from already printed material, historical archives or lawful records. Online removal requests will be assessed promptly.
- Do not provide identifiable member images to sponsors or external marketers for their independent use without an appropriate authority.

14. Direct marketing, fundraising and sponsors

- MEBC may send information about Club activities, membership, events, fundraising and partners where the law and the collection notice allow.
- Provide a clear, functional unsubscribe method for electronic marketing and action opt-outs promptly.
- Do not sell or trade the membership list.
- A sponsor may be acknowledged through MEBC channels, but member contact details must not be disclosed for the sponsor's independent marketing without specific authority.
- Service and safety messages are not marketing and may still be sent when a person has opted out of promotions.

15. Governing bodies and service providers

- MEBC may need to provide information to Baseball NSW, Baseball Australia, competition administrators, insurers, venues, payment providers, registration platforms and other approved providers.
- Before adopting a system, consider what it collects, where data is stored, administrator controls, security, retention, breach support, subcontractors and account closure or export arrangements.
- Provide only the information needed and use contractual, access and configuration controls appropriate to the risk.
- Tell individuals about likely disclosures and overseas handling where required. Internet and cloud services may process data outside Australia even when accessed locally.
- A provider's privacy policy does not remove MEBC's responsibility to choose and configure the service responsibly.

16. Information security

- Use role-based accounts, strong unique passwords and multi-factor authentication for important systems.
- Do not share login credentials through ordinary email or group chat. Use an approved password manager or controlled recovery process.
- Keep devices updated, locked and protected; avoid storing member files on shared family devices or uncontrolled personal cloud accounts.
- Encrypt or otherwise protect sensitive files in transit and at rest where appropriate. Double-check recipients before sending.
- Do not download or print entire databases when a smaller extract will do. Track significant exports and securely delete temporary copies.
- Store paper files in locked storage with controlled keys. Do not leave registration, medical or incident forms visible in vehicles, dugouts or public areas.
- Remove access immediately when a role changes or ends, and review permissions at least each season.
- Report suspicious emails, lost devices, misdirected messages, unauthorised access and unexpected account changes immediately.

Email and spreadsheets

A spreadsheet sent to the wrong address can expose the whole Club. Use the approved system, filter to the minimum fields, verify recipients and avoid attaching full member exports to routine email.

17. Accuracy and correction

- MEBC will take reasonable steps to keep information accurate, complete, current, relevant and not misleading for its use.
- Individuals should update contact, emergency, medical, availability and consent details promptly.
- A correction request should identify the information and proposed correction. MEBC may ask for reasonable verification.
- If MEBC does not make the requested correction, it will explain why and, where required or appropriate, associate a statement of the person's position with the record.

18. Access requests

A person may ask the Privacy Officer for access to personal information MEBC holds about them. MEBC will verify identity and respond within a reasonable period. Access may be provided by inspection, copy, summary or another suitable method.

Access may be limited where lawful and reasonable—for example, to protect another person’s privacy, safeguarding, confidential Board deliberations, legal privilege, an investigation or a serious safety concern. Where possible, MEBC will provide partial access or an explanation rather than refuse the entire request.

19. Retention and secure disposal

- The Board will approve a records-retention schedule covering membership, finance, incidents, health, insurance, complaints, WWCC verification, governance, images and system logs.
- Retention will reflect legal, insurance, governing-body, safeguarding, limitation-period, historical and operational needs.
- Do not keep records indefinitely merely because storage is cheap. Review legacy drives, old email accounts, paper archives and former officials’ devices.
- At the end of retention, securely destroy paper, delete electronic copies and backups where practicable, or de-identify information so a person is no longer reasonably identifiable.
- Suspend routine disposal when information is relevant to a complaint, incident, legal hold, insurance matter, regulator request or investigation.

20. Data-breach response

A person who discovers or suspects a breach must immediately notify the Privacy Officer or President and preserve relevant evidence. Do not conceal the incident or contact affected people independently unless authorised.

MEBC will follow four stages:

Stage	Action
1. Contain	Stop further loss or access: recall a message, disable links or accounts, recover a device, change credentials and isolate compromised systems.
2. Assess	Identify the information, people, cause, access, likely harm and whether remedial action can prevent serious harm. Obtain technical or legal help where needed.
3. Notify	Notify affected individuals, service providers, governing bodies, insurers, Police, regulators or the OAIC where required or appropriate. The Notifiable Data Breaches scheme applies when MEBC is covered by the Privacy Act and the statutory threshold is met.
4. Review	Fix the cause, monitor risk, document decisions, update controls and provide support or guidance to affected people.
Lost or misdirected information Act immediately even if the recipient is trusted or the device has a password. Fast containment can substantially reduce harm and legal risk.	

21. Privacy complaints

- Send a complaint to the Privacy Officer using the contact published by MEBC. If the complaint involves that person, send it to the President or another non-conflicted Board Member.
- Describe the information, event, concern, impact and preferred resolution. MEBC may request identity verification or further detail.
- MEBC will acknowledge, assess and respond fairly within a reasonable period, keep the complainant informed and protect them from retaliation.
- Possible outcomes include explanation, access or correction, apology, deletion, access changes, system improvement, training, provider action or referral under another policy.
- MEBC will advise of any applicable external complaint avenue, which may include the OAIC, NSW Privacy Commissioner, Office of the Children's Guardian or another regulator depending on jurisdiction and subject matter.

22. Roles and accountability

Role	Responsibility
Board	Approves policy, risk settings, major systems, retention schedule and serious breach response; receives de-identified assurance where appropriate.
Privacy Officer / Secretary	Maintains notices and registers, coordinates access/correction requests and complaints, supports training, reviews providers and leads breach assessment.
System owner / administrator	Controls configuration, user access, exports, recovery and audit information for the assigned system.
Coaches and team managers	Use the minimum team and safety information needed, protect it from reuse or disclosure, and return/delete it when the role ends.
All authorised users	Follow notices and controls, access only what is needed, protect credentials and report errors or incidents immediately.
Service providers	Handle information only within their authority and agreed security, retention, support and breach obligations.

Approval and amendment history

Version	Review date	Effective date	Summary
1.0	13/08/26	13/08/26	Comprehensive NSW/Australian replacement of the former Victorian-based policy.

Prepared with reference to current OAIC, NSW privacy and NSW Office of the Children's Guardian guidance. This document is operational guidance and not legal advice.