POLICY | Privacy & Business Intellectual Property

1.0 OBJECTIVE

This policy sets out how Mingara Leisure Group collects, holds, uses, discloses and protects personal information, and how it protects confidential business information and business intellectual property (IP). It also outlines our approach to compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles Privacy Act the Australian Privacy Principles and other applicable legal and regulatory obligations

We do not disclose personal information or confidential business information to third parties for their own direct marketing or independent commercial purposes.

team	safe	reliable	progressive	memorable

we are known for living our values **above the line**	These actions are examples of behaviours that demonstrate our values in practice: I proactively report privacy concerns or breaches I handle personal information and business IP with care, diligence and sound judgement. I do not disclose personal or confidential information inappropriately. I only use approved Microsoft 365 Copilot tools when working with personal information and business IP, and only where that use is consistent with my role and responsibilities. I identify opportunities to strengthen our systems and procedures for handling personal information and business IP.
not living our values is **below the line**	These actions are examples of behaviours and attitudes that do not meet our expected standards: I share others personal information and business IP with people who are not authorised to receive it. I handle personal information and business IP carelessly, including - leaving information - visible on screens or unattended desks. I input personal information or business IP into unapproved public AI tools or large language models I don't report or escalate breaches of this policy

Conduct that does not meet the standards set out in this policy may result in counselling, disciplinary action or other appropriate management action, up to and including termination of employment or engagement.

2.0 SCOPE

This policy applies to personal information collected or held by Mingara Leisure Group in connection with its customers, operations, venues, services, membership activities, business activities and online interactions. It also applies to confidential business information and business intellectual property created, collected, received or held by us in the course of our operations.

Example of personal information may include an individual's name, contact details, membership details, identification details, transaction records, CCTV footage and other information about an identified individual or an individual who is reasonably identifiable.

Examples of confidential business information and business intellectual property may include trade secrets, confidential commercial information, strategic plans, operating procedures, proprietary methods, internal reports and other non-public business information.

We only collect personal information where it is reasonably necessary for our functions or activities, required or authorised by law, or otherwise permitted under applicable law.

3.0 COLLECTION CHANNELS

We may collect personal information directly from individuals , including when they visit our premises, apply for membership, use our services, contact us by phone, email, online, via a third party or through social media, or participate in promotions, events or activities.

We may also collect personal information indirectly, including from publicly available sources, service providers, other organisations, regulatory bodies, exclusion or self-exclusion programs, and other persons where lawful and reasonably necessary.

In some circumstances, you may be photographed, filmed or captured on CCTV footage, at or near our premises or at events or activities conducted or promoted by us. Where identification is required, we may collect or record identification information from documents presented to us, including licences, passports or other identification documents, to the extent reasonably necessary and permitted by law. Where biometric information is collected, the individual will be informed of the nature and purpose of the collection, and any consent required by law will be obtained

We may also create records containing personal information in connection with incidents, compliance matters, observations, complaints, investigations or safety-related matters.

Where reasonably practicable, we take steps at or before the time of collection to notify individuals that personal information is being collected and how it will be handled. We will not collect 'sensitive personal information' which includes things like racial origin or ethnicity, without your consent (but that will often be implied where you choose to provide the information, or you choose to deal with or interact with us where sensitive information might be obtained as outlined in this policy) - except where that is otherwise permissible under the privacy principles.

4.0 ARTIFICIAL INTELLIGENCE (AI) TOOLS AND TECHNOLOGIES

We may use approved artificial intelligence (AI) tools within our secure enterprise environment to assist with internal business tasks such as drafting, summarising, analysis and administrative support.

AI tools are used to support our work and do not replace human judgement or decision-making. All AI-assisted outputs used for business purposes must be reviewed and approved by an authorised person.

Personal information, confidential business information and business intellectual property must only be used with approved AI tools and only in accordance with internal security, privacy and records management requirements.

Approved AI tools must not be used to:

- make solely automated decisions affecting individuals;
- process sensitive information or biometric information except where expressly approved and subject to appropriate legal, privacy and security controls;
- bypass privacy or security controls; or
- input confidential business information into unapproved or public AI platforms.

Where reasonably practicable, personal information should be excluded, anonymised or de-identified before being used with approved AI tools

5.0 VERIFICATION AND IDENTIFICATION

Individuals are required to verify their identity when dealing with us where it is reasonably necessary for security, compliance, operational or legal purposes. If you are not prepared to provide personal information or allow us to collect personal information in our usual way, then we will not be able or may not be prepared to deal with you.

6.0 INTEGRITY AND SECURITY OF PERSONAL INFORMATION

We take reasonable steps to protect personal information ,confidential business information and business intellectual property from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Information may be stored in physical form, electronically, or with secure service providers, including cloud service providers. Where personal information is stored or accessed overseas, we take reasonable steps to ensure appropriate privacy and security protections are in place. Biometric information, where collected, will be stored and managed in accordance with applicable legal, privacy and security requirements.

Access to personal information and confidential business information is restricted to personnel, contractors and service providers who require access for authorised business, legal, compliance or operational purposes and who are subject to appropriate confidentiality obligations.

While we take reasonable steps to protect the information we hold, no method of storage or transmission is completely secure. Individuals should also take reasonable care in relation to their own personal information. If we become aware of an eligible data breach or other serious security incident, we will respond in accordance with our legal obligations, including the Notifiable Data Breaches scheme where applicable

7.0 USE AND DISCLOSURE OF PERSONAL INFORMATION

We use and disclose personal information for the primary purpose for which it was collected, for related purposes that would reasonably be expected, and for other purposes permitted or required by law. These purposes may include providing services, membership services and venue-related services, managing safety, security, compliance and operational matters, verifying identity, administering promotions, events and activities, responding to enquiries, complaints and incidents, meeting legal, regulatory and governance obligations, and communicating with individuals about matters relevant to their relationship with us.

We may disclose personal information to service providers, consultants, contractors and professional advisers who assist us in connection with our operations, to regulatory authorities, law enforcement bodies, courts or tribunals where required or authorised by law, to other organisations involved in exclusion, self-exclusion, compliance or risk management processes where lawful and appropriate, and to other parties where the individual has consented or the disclosure is otherwise permitted by law.

Where personal information is disclosed to third-party service providers , we take reasonable steps to ensure that the information is used only for authorised purposes and subject to appropriate privacy and confidentiality protections. We may also disclose your information to another registered club in connection with an -amalgamation or proposed amalgamation, and to other venues or organisations in -connection with exclusion or self-exclusion arrangements where lawful and appropriate. We may also disclose information where required to maintain statutory registers or meet other legal, regulatory or governance obligations.

8.0 NOTIFICATION AND CONSENT

Where reasonably practicable, we take steps at or before the time of collection to notify individuals about our identity and contact details, the kinds of personal information being collected, the purpose of collection, how the information may be used or disclosed, any usual disclosures to third parties, whether the information is likely to be disclosed overseas, and how the individual may access or correct their personal information or make a complaint.

Where express consent (verbally or in writing, open and obvious) is required by law, we will seek that consent. In some circumstances, consent may be implied from an individual's conduct where that is lawful and reasonable in the circumstances. Sensitive information and biometric information will only be collected, used or disclosed with the required consent or as otherwise permitted by law.

9.0 DATA MINIMISATION AND RETENTION

We take reasonable steps to ensure that the personal information we collect is limited to what is reasonably necessary for our functions and activities. We retain personal information only for as long as it is reasonably required for operational, legal, regulatory, risk management, evidentiary and business purposes, or as otherwise required by law. We review retained information periodically and, where information is no longer required, we take reasonable steps to securely destroy or de-identify it, unless we are required or permitted by law to retain it.

10.0 OPTING OUT

Where lawful and practicable, individuals may opt out of receiving direct marketing communications from us by using the unsubscribe function or by contacting us. Individuals may also request that we do not use or disclose their personal information for certain secondary purposes, although this may not always be possible where the use or disclosure is required for legal, operational, security, safety or membership administration purposes. Some communications, including legal notices, regulatory notices, membership notices and operational communications, cannot be opted out of where they are necessary.

11.0 ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Individuals may request access to the personal information we hold about them and may request correction of that information if it is inaccurate, out of date, incomplete, irrelevant or misleading. Requests for access or correction should be made to our Privacy Officer using the contact details provided in section 14.0 of this policy.

We will respond within a reasonable period and in accordance with applicable law. In some circumstances, access may be refused where permitted by law. If we refuse access or decline to make a requested correction, we will provide written reasons where required.

You also have a right to receive your gaming machine player activity statements to the extent that we are required to provide those under the gaming machines legislation.

12.0 RETENTION OF PERSONAL INFORMATION

Some records are retained for specific periods because of legal, regulatory, evidentiary or operational requirements.

For example, we may collect and retain personal information in registers required under clubs or related legislation, including details relating to temporary members and guests. Those records may include identification information where permitted or required by law. Unless a longer retention period is required or justified, we will generally retain those register records only for so long as is reasonably necessary to meet legal, operational or evidentiary requirements.

13.0 AUSTRALIAN PRIVACY PRINCIPLES (APP) GUIDELINES

In administering this policy, we apply the Australian Privacy Principles Guidelines and relevant guidance issued by the Office of the Australian Information Commissioner.

14.0 PRIVACY ENQUIRIES AND COMPLAINTS

The Privacy Officer has day-to-day responsibility for administering this policy across Mingara Leisure Group's activities and venues.

If you would like to access or correct your personal information, or if you have a question or complaint about how we have handled your personal information, please contact our Privacy Officer using the details set out below. We will acknowledge, assess and investigate privacy complaints within a reasonable period and respond in writing.

If you are not satisfied with our response, you may be able to make a complaint to the Office of the Australian Information Commissioner.

This policy is subject to periodic review and may be updated from time to time. The current approved version is the version published by Mingara Leisure Group from time to time.

The contact details for our Privacy Officer are:

The Privacy Officer
Mingara Leisure Group
12-14 Mingara Drive
Tumbi Umbi NSW 2261
Email: privacy@mingaraleisuregroup.com.au
Telephone: 02 4349 7799

15.0 BREACH OF POLICY

All team members are required to comply with this policy and any related privacy, confidentiality, records management, information security and acceptable use requirements. A breach of this policy may result in counselling, disciplinary action or other appropriate management action, up to and including termination of employment or engagement.

Questions on the interpretation and application or administration of this policy should be directed to the Privacy Officer, General Manager or Human Resources representative, as appropriate.

CONTROL INFORMATION	**Subject**	Privacy and Business Intellectual Property Policy
	Authorised by	Grant Gladman, Chief Executive Officer
	Distribution	All team members
	Original Issue Date	23 October 2001
	Revision Dates	First Issue 23 October 2001 Rev 02 23 January 2018 Rev 03 24 September 2024 Rev 04 23 September 2025 Rev 05 26 May 2026