Hawthorn Football Club PP&OA Privacy Policy

Applies to:	Hawthorn Football Club Past Players & Officials Association (HFCPPOA, we us, our)
Last Updated	3 July 2026
Approved by:	John Hook (Secretary)

This Privacy Policy explains how Hawthorn Football Club PP&OA (HFCPPOA) collects, holds, uses and discloses personal information, and how you can access and correct your personal information or make a privacy complaint.

We are committed to handling personal information in accordance with the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**.

---

1. Scope and how this policy works

1.1 Who this policy covers

This policy applies to individuals whose personal information we manage, including (as relevant):

members and prospective members; ticket purchasers and event attendees; participants in programs, events, and community activities; donors, sponsors, corporate partners and their representatives; customers of our services and products (including online services); website and app users; volunteers and contractors; and people who contact us with enquiries or complaints.

1.2 Employee records

Where applicable, employee records may be exempt from some requirements of the Privacy Act where the employee records exemption applies.

1.3 When other policies may apply

Where we engage third-party platforms or service providers (for example, ticketing, payments, events, streaming, marketing platforms or identity verification providers), their privacy policies may also apply to their handling of your information.

---

2. What is “personal information” and “sensitive information”?

2.1 Personal information

“Personal information” means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

2.2 Sensitive information

“Sensitive information” includes certain categories of personal information that receive higher protection under the Privacy Act, such as health information, biometric information, racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual orientation and criminal record.

We will generally only collect sensitive information where:

You consent and it is reasonably necessary for our functions or activities; or collection is otherwise permitted by law.

---

3. The kinds of personal information we collect and hold

Depending on your relationship with us, the types of personal information we may collect include:

3.1 Identity and contact details

Name, date of birth/age, postal address, email address, telephone number; membership number and membership history.

3.2 Transaction and engagement information

Credit/debit card information, purchases (e.g., tickets, memberships, merchandise), payment confirmations and related administrative records; event attendance history and participation information (e.g., program registrations); preferences (e.g., seating preferences, communications preferences, club support preferences); competition, promotion and survey participation.

3.3 Online and device information

Website/app usage information (e.g., pages viewed, time and date of visits, referrers); device identifiers and technical data (e.g., IP address, browser type, device type); cookies and similar tracking technologies (see Section 11).

3.4 Health and safety information (where relevant)

Accessibility requirements; incident and injury details (where relevant to an event, venue access, or safety incident); public health information where required for lawful public health or venue entry purposes.

3.5 Images, audio and video

Photographs, video and audio recordings at events, activities and in/around premises; CCTV footage (see Section 9).

4. How we collect personal information

We collect personal information in a range of ways, including:

4.1 Directly from you

When you:

Purchase tickets, memberships or merchandise; register for events, programs or services; enter competitions or promotions; complete surveys or provide feedback; create or use an account on our platforms; or contact us (including by phone, email, online forms or in person).

4.2 Automatically through digital channels

When you use our websites, apps, Wi-Fi services (where offered), or interact with our digital content, we may collect information via cookies, pixels, SDKs and similar tools (see Section 11).

4.3 From third parties

We may collect personal information from:

The Hawthorn Football Club, AFL, state leagues, clubs, venues, ticketing agencies and event delivery partners (where relevant to your engagement with the HFCPPOA; service providers (e.g., payment processors, marketing platforms, analytics providers, identity verification providers); publicly available sources; and other third parties where you have consented or where collection is permitted by law.

---

5. Why we collect, hold, use and disclose personal information

We collect, hold, use and disclose personal information for purposes connected with our functions and activities, including:

5.1 Membership, ticketing, products and services

Processing membership, ticketing and merchandise transactions; delivering services, benefits and entitlements; administering events, programs, promotions and competitions.

5.2 Communications and relationship management

Responding to enquiries and complaints; sending service/administrative communications (e.g., renewal notices, event changes, account notifications); maintaining and improving our relationships with members, supporters, customers, donors, sponsors and partners.

5.3 Marketing and promotional communications

Sending you news, offers, promotions, surveys and other marketing communications (including from sponsors/corporate partners where applicable and permitted).

You can opt out of marketing at any time (see Section 12). Opting out may be list-specific and you may still receive essential administrative messages.

5.4 Health & well-being services

Understanding information about your health and well-being for the purposes of our past players and officials' health and well-being services including the player hardship fund or similar services. We will generally ask for your further consent to manage your health or other information which is considered sensitive under applicable privacy and data protection laws.

5.5 Improvement, analytics and operational management

Understanding how our services are used; improving our platforms, offerings and supporter experience; internal reporting, auditing, risk management and governance; fraud prevention and security monitoring.

5.6 Safety, security and compliance

Maintaining a safe environment at venues and premises; managing incidents and investigations; complying with legal and regulatory requirements and responding to lawful requests (see Section 8).

5.6 Research and insights (including AI-assisted analysis)

Analysing survey responses and feedback, including sentiment analysis and trend identification; generating operational insights and improving communications (see Section 10).

---

6. When we disclose personal information

We may disclose personal information to the following categories of recipients (as relevant):

6.1 Service providers and contractors

Including providers who assist with:

IT and cloud services; data storage and hosting; marketing, CRM and communications distribution; analytics and measurement; ticketing, payments and fraud detection; customer support; and event and venue operations.

6.2 Event and program stakeholders

Where relevant, we may disclose limited participant information to:

Venues and event delivery partners (for access, logistics and safety); presenters, facilitators and program partners; sponsors/corporate partners where you have agreed or where permitted (e.g., where a partner benefit is delivered).

6.3 Related bodies and sporting administration

Where relevant to delivery of HFCPPOA related programs and services, we may disclose information to bodies involved in administration, competition operations, integrity and safety functions.

6.4 Legal and regulatory disclosures

We may disclose personal information where required or authorised by law, including to:

Law enforcement agencies; courts and tribunals; regulators and government agencies; and professional advisers (e.g., lawyers, auditors) under confidentiality obligations.

---

7. Overseas disclosures

Some of our third-party service providers may store, process or access personal information from outside Australia (for example, where cloud infrastructure or support teams are located overseas).

Where we disclose personal information overseas, we will take reasonable steps to ensure the overseas recipient manages the information in a manner consistent with the Australian Privacy Principles, unless an exception applies under the Privacy Act.

---

8. Security of personal information

8.1 Our security approach

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Our safeguards may include:

Access controls and user authentication; encryption in transit and, where appropriate, at rest; network security monitoring and vulnerability management; logging and audit trails for key systems; segregation of duties and least-privilege access practices; staff training and confidentiality obligations; and vendor due diligence and contractual controls for service providers.

8.2 Data breaches

If we become aware of an eligible data breach, we will assess and respond in accordance with the **Notifiable Data Breaches scheme**, including notifying affected individuals and the OAIC where required.

---

9. CCTV and physical security

9.1 Use of CCTV

We may use CCTV at or around our premises and at Hawthorn Football Club controlled locations for:

Safety and security; incident detection and investigation; protection of staff, members, visitors and assets; and compliance with legal obligations.

9.2 Storage and access

CCTV footage is stored securely and access is restricted to authorised personnel or contracted security providers as required for their functions. We may provide CCTV footage to third parties (e.g., venue operators, police, insurers, legal advisers) where required or authorised by law or where necessary to investigate an incident.

9.3 Retention of CCTV footage

Unless required for an investigation, legal proceedings or regulatory compliance, CCTV footage is typically retained for a limited period appropriate to operational needs and then securely deleted or overwritten.

9.4 Access requests for CCTV

Requests for access to CCTV footage will be considered on a case-by-case basis. We may refuse access where permitted by law, including where granting access would unreasonably impact the privacy of other individuals or prejudice an investigation.

---

10. Artificial intelligence (AI) and automated processing

We may use AI-enabled tools to support our operations and improve services. This section explains how we do so and the safeguards we apply.

10.1 How we may use AI

We may use AI tools for purposes such as:

Generating transcripts, summaries or notes from meetings, calls or events where recording/transcription is used; analysing survey responses and feedback (including sentiment analysis and topic clustering); personalising content or communications (e.g., tailoring messages based on preferences and engagement); detecting anomalous activity for security and fraud prevention (e.g., unusual account activity signals).

10.2 What information may be used

Depending on the use case, AI tools may process:

Contact and engagement information; content of communications you send us (e.g., enquiry text); survey responses and feedback; audio/video recordings where used for transcription or safety purposes; and technical and usage data from our digital platforms.

10.3 Human oversight and decision-making

We aim to apply human oversight for material decisions that affect individuals, particularly where decisions could have a significant impact (e.g., account restrictions, fraud outcomes, complaint decisions). If an AI-enabled tool is used to generate content or insights, we treat outputs as support tools and apply review processes appropriate to the context.

10.4 Safeguards for AI use

We take reasonable steps to ensure AI use is managed appropriately, which may include:

Limiting data provided to AI tools to what is reasonably necessary; applying contractual and technical controls with AI vendors, including confidentiality and security requirements; configuring tools to reduce retention of prompts/inputs where feasible; restricting access to AI tools and outputs; and monitoring and periodically reviewing AI use cases.

---

11. Cookies, analytics and online tracking

11.1 Cookies and similar technologies

We may use cookies, pixels, SDKs and similar technologies to:

Operate our websites and apps; remember preferences; measure performance and usage; and improve content and supporter experience.

11.2 Managing cookies

You can manage cookies through your browser settings and, where available, through our cookie preferences tools. Blocking some cookies may affect site functionality.

---

12. Direct marketing and your choices

12.1 Marketing communications

We may send marketing communications by email, SMS, push notification or other channels where permitted.

12.2 Opting out

You can opt out by:

Using the unsubscribe function in an email; adjusting communication preferences in your account (where available); or contacting us using the details in Section 15.

Even if you opt out of marketing, we may still send important administrative messages (e.g., membership servicing, ticketing confirmations, program notices, policy updates).

---

13. Retention and destruction of personal information

We take reasonable steps to retain personal information only for as long as needed for the purposes described in this policy unless we are required or authorised by law to retain it longer.

13.1 Typical retention approach (guidance only)

Retention periods vary depending on context, but we generally apply the following approach:

Membership records: retained for the duration of your membership and for a reasonable period afterwards for administration, dispute resolution, legal compliance and auditing.

Ticketing and transaction records: retained in accordance with legal, accounting and tax requirements and for a reasonable period for customer support and dispute handling.

Program participation records: retained for the duration of the program and a reasonable period afterwards for administration, incident management and compliance.

Marketing preference records: retained to respect your choices and to maintain suppression lists (so we do not re-add you contrary to your opt-out).

Website/app logs and analytics: retained for periods consistent with security, fraud detection and platform improvement needs.

CCTV footage: retained for a limited period and overwritten/deleted unless required for investigations or legal reasons (see Section 9).

13.2 Secure disposal and de-identification

When personal information is no longer required, we take reasonable steps to securely destroy it or de-identify it (subject to legal requirements).

---

14. Access and correction

14.1 Access requests

You may request access to personal information we hold about you by contacting us (see Section 15).

We will:

Respond within a reasonable time (generally within **30 days** where practicable); ask you to verify your identity before releasing information; and provide access in the manner requested where reasonable and practicable.

We may charge a reasonable administrative fee for providing access (but not for making the request).

14.2 When access may be refused

We may refuse access where permitted by law (for example, where granting access would unreasonably impact the privacy of others, prejudice an investigation, or where legal privilege applies). If we refuse, we will provide reasons where required and explain available complaint avenues.

14.3 Correction requests

If you believe personal information we hold is inaccurate, out of date, incomplete, irrelevant or misleading, you may request correction.

We will take reasonable steps to correct the information. If we do not agree the information should be corrected, we will (where required) take reasonable steps to associate a statement with the information noting your request.

---

15. How to contact us

To make a privacy enquiry, request access/correction, or make a complaint, contact us via our official contact channels listed on the HFC PP&OA website or by writing to our Privacy Officer through the Club's published contact details.

https://hawthornpastplayers.com/index.php/contact-us/

(We do not publish personal email addresses or direct phone numbers in this policy.)

---

16. Complaints

16.1 Making a complaint

If you have a complaint about how we manage personal information, contact us with details of your concern. We may ask for additional information to help investigate.

16.2 Our response

We will acknowledge and investigate complaints and aim to respond within a reasonable timeframe.

16.3 OAIC

If you are not satisfied with our response, you may contact the **Office of the Australian Information Commissioner (OAIC)** to make a complaint or seek guidance.

Office of the Australian Information Commissioner (OAIC) – *Privacy complaints*

---

17. Changes to this policy

We may update this Privacy Policy from time to time. The updated version will be published through our official channels and will apply from the “Last updated” date shown at the top.