

MINCHINBURY JETS SOCCER CLUB APP

Privacy Policy

Your information. Your club. Your control.

Version 1.2

Effective 28 July 2026

Minchinbury Jets Soccer Club Incorporated

ABN 95 372 250 224

Minchinbury Oval, 22 Minchin Drive, Minchinbury NSW 2770

Privacy contact: mjsc@outlook.com.au

www.minchinburyjets.com

Privacy at a glance

The App supports a community football club, including families, child players and junior referees. This page summarises the Club's core privacy promises; the detailed sections that follow control if more detail is needed.

Private by default Home addresses, emergency contacts, payment records and private messages are not visible to ordinary users. Access depends on account ownership, a verified family link, team role or authorised committee duty.	Junior safeguards Under-18s cannot create a normal account. The only child access is a restricted junior view-only account linked through a parent or guardian, with no messaging, purchasing, RSVPs or shop access.
No live location The App does not request, collect or track precise device location. Venue pins are fixed locations. A separate maps app may use location if the user chooses and permits it.	No medical records The App does not collect medical conditions or allergies. It may hold two emergency contacts for a player, including name, phone and email.
Protected payments Square handles full card details. The App keeps only limited payment records such as brand, last four digits, expiry, status, receipts and Square references.	No analytics or tracking The App contains no analytics, advertising or cross-app tracking SDKs. The Club does not sell personal information or give sponsors a member contact list without permission.

Who can ordinarily see what

Information	Ordinary visibility
Private messages	Only the sender and intended recipient(s) or group participants. A committee role does not permit routine browsing of private messages.
Player administration	The adult player or verified linked parent/guardian, plus authorised committee members who need the information for club duties.
Home address and emergency contacts	Not visible to teammates or ordinary users. Available only to the individual or linked guardian and authorised committee members for administration or safety.
WWCC records	The person whose check it is and the MPIO or CSO responsible for the restricted WWCC register.
Complaints	The MPIO and CSO only, except where limited technical or lawful access is required.
Team participation	Linked family and approved team officials receive the information needed for team activities. A junior view-only account sees only its team, fixtures and Golden Boot information.
Payments	The payer and authorised registration, finance or committee users. Square receives card details.

Contents

Privacy at a glance	2
1. About this policy	4
2. Who is responsible	4
3. App users and access areas	4
4. Personal information we collect	4
5. Information we do not collect or retain	6
6. How we collect information	6
7. Why we use personal information	7
8. Access controls and who can see information	7
9. Children, junior players and junior referees	8
10. Payments, forms, vouchers and emails	9
11. Device permissions and local storage	10
12. Service providers and overseas recipients	10
13. When we disclose personal information	11
14. How we protect information	11
15. Retention, account deletion and de-identification	12
16. Access, correction and privacy choices	12
17. Notifications and Club communications	13
18. Data incidents and breach response	13
19. Privacy enquiries and complaints	13
20. Third-party links and independent services	13
21. Changes to this policy and contact	14
A. Main service providers	14
B. Legal and guidance references	15

1. About this policy

This Privacy Policy explains how Minchinbury Jets Soccer Club Incorporated (the Club, we, us or our) collects, holds, uses, discloses and protects personal information through the Minchinbury Jets Soccer Club App (the App). It also explains who can see information, how connected providers process it and the choices available to users.

The policy applies to the mobile App, shared signed-in and role-restricted areas, committee and administration functions, related web views, authorised registration imports, referee applications, payments, emails and the connected services named below. It covers parents and guardians, adult players, child players, coaches, managers, volunteers, referees, committee members, event attendees, customers, sponsors and other people whose information is handled through the App.

The Club aims to manage personal information consistently with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), applicable NSW laws and recognised child-safe practices, to the extent those requirements apply. The promises in this policy are also the Club's operational standard for the App.

Plain-language priority

If a shorter collection notice shown inside the App conflicts with this full policy, the Club will prefer the interpretation that gives the clearer privacy protection, subject to law and the App's actual technical operation.

2. Who is responsible

The organisation responsible for the App and Club-controlled information is:

Minchinbury Jets Soccer Club Incorporated

ABN 95 372 250 224
Minchinbury Oval, 22 Minchin Drive, Minchinbury NSW 2770
Privacy email: mjsc@outlook.com.au
Website: www.minchinburyjets.com

The Club Committee oversees privacy governance. Administrative access is assigned according to committee responsibility. Connected providers may process information for the Club or under their own terms, as described in sections 10 to 12 and Appendix A.

3. App users and access areas

Shared signed-in areas

Signed-in users may see audience-targeted announcements, fixtures, events, sponsors, approved committee contact fields, Club documents and insurance information. Shared content must not include home addresses, emergency contacts, private committee contact details, WWCC records, complaints, private messages or payment records.

Member and role-restricted areas

Every account is authenticated and receives permissions according to account ownership, verified family link, assigned team, approved registration and Club role. Account types include parent or guardian, adult player, coach or manager, committee, and the restricted junior view-only option. Features and data access differ by role.

No normal child accounts

A person under 18 cannot create a normal App account. Sign-up checks the entered name against Club registration records and blocks normal account creation if the only match is an under-18 player. A parent or guardian must create the family account and link the child. The only child access is a restricted junior view-only account with the limits described in section 9. Shared and private App functions require an authenticated account.

4. Personal information we collect

The exact information depends on the person's role and the functions used. The following inventory is intended to name all current categories, including records about children. A field may be blank when optional or not relevant.

Person or feature	Information collected or processed
Every account	Full name; email address; mobile phone number; authentication status; account type; linked players, teams and roles; security and verification records. A password is supplied to Firebase Authentication for sign-in. The Club does not receive, display or store a readable password in Firestore.
Player identity	First, middle and last name; date of birth; gender; season; home or postal address where included in registration data; Play Football Participant ID; FFA number; player email and mobile; general contact email and phone; registration and verification details.

Person or feature	Information collected or processed
Parents and family	Parent or registrant name, mobile and email; relationship or authority to act; family group name; linked family members; account-matching information; six-digit linking-code status and registered contact channel.
Emergency contacts	Up to two emergency contacts for a player, including name, phone number and email address. The App does not collect medical conditions or allergies.
Registration and money owed	Team and age group; registration status; approval or payment status; fees payable; amounts paid and owing; discounts or adjustments; payment-plan and instalment details; desk-payment confirmations; receipts and related notes needed to reconcile registration.
Football participation	Assigned team; coach and manager assignments; season; availability and attendance answers; reasons provided with an answer; lineup and field positions; formation information; goals scored and Golden Boot totals; award wins; match or referee-entered results.
Coaches, managers and volunteers	Name; date of birth; email; phone; role; Working With Children Check (WWCC) number and expiry; verification or compliance status; team assignments; game-day or volunteer availability; authorised administrative notes.
Committee members	Name; role or roles; public club-role email; optional approved photo; short description; private mobile and personal email used for account matching; game-day availability including times, positions and reasons. Private personal email and mobile are not displayed to other users.
MiniRoo referees	Name; optional date of birth; parent or guardian name, email and phone; availability; field preferences where supplied; game assignments; fees earned; payment status; and results entered. A junior referee is managed through a parent or guardian account and may use only the restricted junior view-only option if the Club enables it.
Referee applications	Information submitted through the Jotform referee application: applicant name, date of birth, phone, email, under-18 indicator, parent or guardian details and preferred field or age-band information requested on the form.
Card and payment records	Buyer or payer name and email; player name included in a payment note; item, registration or event; amount; date; status; refunds; receipt; Square customer, payment, order or saved-card reference IDs; and, where returned by Square, card brand, last four digits and expiry. Full card numbers and security codes are not stored by the App.
Chats and messages	Team and committee chats and direct messages: sender name, role, text, date and time, intended recipients or conversation membership, reactions, delivery-related metadata and any content deliberately included by a participant.
Events and tickets	RSVP name; attendee count; optional dietary requirements; event or ticket selection; order and payment status; QR ticket identifier; ticket holder name and email; check-in or redemption status; and event photographs an authorised committee or admin user deliberately uploads.
Complaints	Complaint text, category, date, status, attachments or follow-up records supplied through the function. A complaint may be submitted without a name. Complaint content is restricted to the Member Protection Information Officer (MPIO) and Child Safety Officer (CSO), subject to lawful or essential technical handling.
Sponsors and shop content	Sponsor business name, logo, business address, public business contacts and approved sponsor information; product names, descriptions, prices, variants and images uploaded by an authorised committee user. Business contact details may be personal information for a sole trader or individual contact.
Uploaded media	Event photographs, sponsor logos and gear or uniform product images deliberately selected by an authorised committee or admin user. Selected files are uploaded to the Club's Firebase Cloud Storage; the App does not browse or upload the rest of the photo library.
Device and local data	Push-notification token saved against the account in Firestore when permission is granted; an authorised offline cache of App data; session state; cart contents; saved-card reference; notification read state; QR or barcode scan text; selected calendar-event details; and a specific image deliberately chosen for upload.
Address search	Typed address text sent to the configured OpenStreetMap-based geocoding service when an authorised user uses address autocomplete to create an event. The App does not send the device's live GPS location.
Provider technical data	The App and its providers may automatically process IP address, request time, device or operating-system type, App version, authentication events and limited network, delivery, error or security logs needed to provide and protect the service. An approximate area may be inferred from an IP address; precise device location is not collected. The App contains no analytics, advertising or tracking SDK.
Public competition data	Public Dribl fixtures, results, tables, grounds, team names and match information displayed or linked in the App. The Club does not send personal information to Dribl merely to retrieve public fixtures.

Sensitive and high-risk information

The App does not maintain player medical-condition or allergy records and is not intended to collect racial or ethnic origin, biometric templates or other unrelated sensitive information. An optional event dietary requirement may incidentally reveal health or religious information; when a user chooses to provide it, the Club uses it only to organise the requested event or catering. WWCC, complaint, child-safety, child contact and identifiable event-photo records are treated as high-risk personal information even where a legal definition may differ. Users should not put unnecessary sensitive information into a chat, complaint, image or free-text field.

5. Information we do not collect or retain

- No normal child accounts: an under-18 registration match is blocked from normal sign-up. The only child option is a restricted junior view-only account; it has no messaging, ticket buying, RSVPs or shop access.
- No precise live location: the App does not request, read, collect or track GPS or other precise device location.
- No microphone, contacts, biometrics or recording: the App does not use the microphone, device contacts, fingerprint or face data, or audio or video recording.
- No medical or allergy records: the App does not collect or store medical conditions, injuries, treatments or allergies.
- No readable Club password record: Firebase Authentication processes account credentials; the Club cannot see a user's readable password.
- No full card credentials: the App does not store a full card number, card security code, online-banking credential or full bank-account credential.
- No retained voucher code: the current Service NSW connection is sandbox-only. A scanned or typed Active and Creative Kids voucher code is sent with the child's name and date of birth to the configured test service and is not stored in Firestore or retained by the App after the response.
- No camera photographs: camera frames are used only to read event-ticket or Active and Creative Kids voucher QR or barcode text and are not captured, uploaded or saved as photos.
- No reading of existing calendars: the App adds only an event the user chooses and does not intentionally read or upload the user's existing calendar entries.
- No analytics, tracking, advertising profile or sale: the App contains no analytics or tracking SDK, and the Club does not sell personal information, track users across unrelated apps or create behavioural advertising audiences.

Provider records are separate

A third party may keep information under its own notice. Square keeps payment and anti-fraud records, Jotform processes form submissions, the configured Service NSW sandbox may log test requests, and email, geocoding or push providers keep delivery and security logs. This does not mean the Club stores full card details, voucher codes or precise location in Firestore.

6. How we collect information

- Directly from a person when they register, sign in, edit an account, link a player, send a message, respond to availability, submit a complaint or form, RSVP, scan a code, add an event, order an item, make a payment, enter a voucher or seek support.
- From a parent or guardian who provides or verifies information for a child player or junior referee.
- From an authorised committee member who imports a registration report, creates a team, assigns a role, verifies a WWCC, records a desk payment, enters an award or result, or corrects Club information.
- From authorised PlayFootball or other football registration reports and spreadsheets supplied to the Club.
- From Square, the Service NSW sandbox, Brevo, Dribl and other connected providers when a user deliberately uses the relevant function or the provider returns a status or reference. Referee application information is entered directly into Jotform and may later be made available to authorised Club users.
- When an authorised committee or admin user deliberately selects an event photo, sponsor logo or gear image for upload to Firebase Cloud Storage.
- When an authorised user types an event address into autocomplete; the typed address text is sent to the configured OpenStreetMap-based geocoding service.
- Automatically from Firebase, Cloudflare, Expo, Apple, Google or the user's device for authentication, backend operation, notifications, network security and reliable delivery. The App does not run analytics or tracking SDKs.

A person providing information about somebody else must be authorised to do so and should make that person aware of this policy. Parents and guardians are responsible for providing accurate information about linked children.

7. Why we use personal information

- Create, verify, secure and manage accounts, family links, team assignments and role permissions.
- Confirm identity, registration, eligibility, payment status, amounts owing and access to Club functions.
- Manage teams, coaches, managers, training, attendance, lineups, positions, formations, results, goals, awards and game-day duties.
- Run the MiniRoo referee program, including applications, parent contact, availability, assignments, entered results and fees earned.
- Provide private team, direct and committee communication, and deliver approved Club notices.
- Manage events, RSVPs, dietary requests, tickets, QR check-in, authorised event photos, uniforms, shop images and orders, desk payments, card payments, refunds and receipts.
- Send fee reminders containing player names and amounts owing, password-recovery messages, account-linking codes and FFA reminders through Brevo from mjsc@outlook.com.au.
- Send a voucher code, child's name and date of birth to the configured Service NSW sandbox to test Active and Creative Kids validation or redemption, without storing the code in Firestore.
- Use Cloudflare backend services for payment plans, shop refund requests and game-day duty rosters.
- Send a typed event-address query to an OpenStreetMap-based geocoding service to return address suggestions.
- Verify WWCC compliance and support child-safety, safeguarding, complaints, emergencies and conduct processes.
- Provide public fixtures and results from Dribl without sending Club personal information to Dribl for that retrieval.
- Send push notifications through Expo, including announcements, fixture changes, fee reminders and auto-debit receipts; a payload may contain a player name or payment amount.
- Prevent unauthorised access, fraud or misuse; troubleshoot service delivery; and maintain proportionate security records.
- Comply with law, court orders, insurance requirements and authorised football or association rules.
- Prepare de-identified or aggregated participation, referee, award or financial reports for Club operations.

Human review of significant decisions

The App may suggest family matches, team placement or data-quality checks. An authorised person reviews decisions that materially affect registration, access, payment status or participation. The Club does not rely solely on an algorithm for a legal or similarly significant decision.

8. Access controls and who can see information

The App uses Firebase Authentication, Firestore security rules, backend checks and role-based permissions. A record may be available because the user owns it, is a verified parent or guardian, is assigned to the relevant team or conversation, or has an authorised committee responsibility.

Person or role	Permitted access
All signed-in users	Audience-targeted announcements, fixtures, events, sponsors, approved committee contact fields, Club documents and insurance information.
Parent or guardian	Own account and linked children's records, team chat, availability, fees and payment plans, tickets and uniform shop. A parent cannot search for or link an unrelated child without verification.
Restricted junior view-only	Own team, fixtures and Golden Boot information only. No messaging, ticket buying, RSVPs or shop. An availability change requires parent or guardian approval before it takes effect.
Adult player	Own player record, assigned team and team chat, availability, fees and payment plans, tickets and uniform shop.
Coach or manager	For the assigned team: lineups, results, training requests, gear sign-out and team-chat pins. Team Officials chat is available only after the coach or manager registration is Approved.
Registrar	Rosters, registration imports and fee settings needed for registrar duties.
Treasurer	Payment administration, payment plans, transaction records and desk-payment confirmations needed for treasury duties.
Uniform Officer	Gear hub, uniform orders, relevant buyer and player details, and shop refund requests needed for fulfilment and refunds.
Secretary	Referee administration, photo-day records, training allocation and authorised exports needed for secretary duties.

Person or role	Permitted access
MPIO and CSO	Restricted complaint, safeguarding and WWCC-register information. Complaints are not visible to the general committee or ordinary users.
President and Secretary	Announcements and season-handover functions, together with information reasonably needed for those duties.
Committee chat member	Committee chat only while assigned to the authorised committee conversation. A committee title does not provide access to unrelated direct or team messages.
Message participant	Only messages and reactions in a direct or group conversation to which the account belongs.
Junior referee's parent	The junior referee profile, availability, assignments, entered results and fees managed through the parent's verified account.
Signed-in directory user	Only approved directory fields: name, Club role, Club-role email, optional photo and description. Private personal email and mobile are not displayed.
Technical administrator	Exceptional backend access only where reasonably necessary for security, support, recovery, legal compliance or child safety, and then only with confidentiality and least-access controls.
Service provider	Only the information its service needs, under the provider's terms and the Club's configuration. Provider personnel do not receive a general Club role.

Private messages

Direct and group messages are visible only to their intended participants. Other users cannot search or read them, and a committee title does not provide routine message access. Information may be preserved or accessed in an exceptional case where technically and legally necessary to investigate a reported safety issue, prevent serious harm, respond to a valid legal demand, resolve a security incident or enforce Club rules. Any such access must be limited and recorded where practicable.

Home addresses, emergency contacts and WWCC

These fields are not displayed to team members or ordinary users. Home addresses and emergency contacts are restricted to the person or verified guardian and authorised committee duties. WWCC number, expiry and verification status are visible only to the check holder and the MPIO or CSO responsible for the restricted WWCC register.

9. Children, junior players and junior referees

The App handles children's personal information because the Club runs junior football and a MiniRoo referee program. Children's information receives heightened protection and is used only for genuine Club, team, registration, payment, referee, communication and safety purposes.

- A person under 18 cannot create a normal App account. Sign-up checks the typed name against Club registration records and blocks normal account creation when the only matching player is under 18.
- A parent or guardian must create the main account and link the child. A child can use only a restricted junior view-only account if the Club enables that option.
- A restricted junior view-only account can see only the child's team, fixtures and Golden Boot information. It cannot use any direct, team, committee or officials chat.
- A restricted junior view-only account cannot buy tickets, submit RSVPs or use the shop. Any availability change requires parent or guardian approval before it is accepted.
- A parent links a child using an emailed six-digit verification code sent to the registered address. Codes should not be shared.
- Junior referees are managed through a verified parent or guardian account. The Club may store the referee's name, optional date of birth, parent contacts, availability, assignments, entered results and fees.
- Stored child-player information includes name, date of birth, gender, team, fees, parent and emergency contacts, goal or Golden Boot tallies and, for a junior referee, referee availability and parent contacts.
- FFA numbers are sent only to the registered email address for the relevant reminder and are not displayed on screen in the App.
- A child player's home address, emergency contacts, registration identifiers and financial details are not visible to teammates or ordinary users.
- Assigned team officials and team members may see only information needed for participation, such as name, team, availability, position, lineup, goals or awards.
- The App stores no child medical-condition or allergy record. An optional dietary note on an event ticket may reveal health information and is restricted to organising that event.

- An authorised committee or admin user may upload an event photograph to Firebase Cloud Storage. The Club must obtain and follow any required media consent and child-safety process before using an identifiable child's image.
- A verified parent or guardian may request access, correction, unlinking or deletion of a child's App information, subject to identity checks and lawful retention.

Children's Online Privacy Code

As at 28 July 2026, the Australian Children's Online Privacy Code is still being developed and must be finalised and registered by 10 December 2026. The Club will review this policy and the App's child-privacy controls when the Code is registered and before any compliance date that applies.

10. Payments, forms, vouchers and emails

Square card payments and shop

Checkout and receipt functions open Square's pages or forms. Card details go directly to Square's secure payment environment and vault and never touch the App or Club database. The App may keep card brand, last four digits, expiry and Square customer, payment, order or saved-card reference IDs, together with amount, item, status, date, refund, instalment and receipt information. Buyer name and email, and a player name included in payment notes, are sent to Square. Square separately retains payment, fraud-prevention and compliance information under its privacy notices.

Payment plans, instalments and desk payments

The App and Cloudflare backend may process a buyer name and email, player name, saved-card reference, card brand and last four digits, payment-plan schedule, instalment amount and due date, amount paid or owing, status, manual or desk-payment confirmation, confirming committee user, receipt and reconciliation notes. These records do not contain a full card number.

Active and Creative Kids vouchers

The Service NSW connection is currently sandbox-only. When a user tests validation or redemption, a scanned or typed voucher code, child's name and date of birth are sent to the configured Service NSW test service. The code is not stored in Firestore or retained by the App after the response. If live redemption is enabled later, this policy and the in-context collection notice must be reviewed before launch.

Jotform referee applications

The referee application form opens Jotform and asks for the applicant's name, date of birth, phone, email, under-18 indicator, parent details where required, and field or age-band preference. Information entered on that form goes directly to Jotform; the required application record is then stored in Firebase for authorised Club users. The form must not be used for card details, medical information or unrelated sensitive information.

Brevo club email

Brevo sends Club emails from mjsc@outlook.com.au, including fee reminders containing player names and amounts owing, password-recovery messages, family-linking codes and FFA reminders. The Club sends the recipient name and registered email address plus the required message content. A readable password is never disclosed, and an FFA number is sent only to the registered address and is not shown in the App. Email is not a secure place to send passwords, full card details, voucher codes or unnecessary personal information.

11. Device permissions and local storage

Permission or data	How it is used
Push notifications	With permission, the App saves the phone's push token against the person's account in Firestore and uses Expo and the device platform for announcements, fixture changes, fee reminders and auto-debit receipts. A payload may contain a player name or payment amount and may appear on a locked screen.
Camera	Used only for event-ticket and Active and Creative Kids voucher QR or barcode scanning. No photo is taken or stored; only the decoded code text is used.
Photo library	Committee or admin only. The user deliberately selects an event photo, sponsor logo or gear or uniform product image for upload to Firebase Cloud Storage. The App does not inspect or upload the rest of the library.
Calendar	Write-only. The App adds a Club event the user has chosen to RSVP to and does not read or upload existing calendar entries. The web version may open Google Calendar to add the selected event.
SMS composer	The field-lights screen pre-fills a text message and lighting-controller phone number in the device's SMS composer. The App does not send it automatically; the user must review it and press send.
Maps and location	The App does not request or use GPS or device location. Maps show fixed venue pins. If a user opens Apple Maps or Google Maps, that independent app may use location under its own settings.
Local device storage	May hold an authorised offline cache of the same App data the user can access, session state, cart, saved-card reference and notification read state. Logout, clearing App data, account deletion or uninstalling may remove some or all local data.
Not used	Microphone, contacts, biometrics, audio recording and video recording are not requested or used.
Analytics and tracking	The App contains no analytics, advertising or cross-app tracking SDKs.
Network and security	Firebase, Cloudflare, Expo and platform services may receive IP address, device or operating-system type, App version, request time and limited delivery or security logs. Approximate area may be inferred from IP.

Permissions can be changed in device settings. Refusing an optional permission limits only the related function where technically possible; for example, refusing camera access prevents scanning but should not prevent ordinary account use. Because the offline cache may contain child, team or payment information the signed-in user is authorised to see, users should secure the phone with a device passcode and sign out before sharing or disposing of it.

12. Service providers and overseas recipients

The Club uses the providers listed below to run the App. Most are global services and some personal information is likely to be processed outside Australia. Appendix A gives the function, information involved, likely location and provider privacy link.

Provider	Likely overseas processing or location position
Google Firebase	The minchinbury-jets-soccer-club project uses Firebase Authentication, Firestore and Cloud Storage. Authentication is processed in the United States; database and storage location depend on the Club's configured regions; Google may also process globally.
Cloudflare	Cloudflare processes payment-plan details, shop refund requests, duty rosters, API traffic and security logs. It states that it primarily stores information in the United States and European Economic Area and may transfer or access it globally.
Square	Square processes buyer and payment information, including buyer name and email and a player name in payment notes. Its Australian notices identify the United States, Canada, Japan, Ireland, France, Spain and the United Kingdom among overseas processing or storage locations.
Brevo	Brevo processes recipient names, emails, player names, amounts owing and message content. It states that its main database hosting is in the European Union, including France, Germany and Belgium; other subprocessors may be elsewhere.
Jotform	Standard form data is stored in the United States unless the Club has selected another available data region. Australian data may be handled by US-based cloud providers.
Expo	Expo may transfer and process App end-user information in the United States, including push tokens and payloads that may contain a player name or payment amount.
Apple and Google	Push delivery data and user-directed Maps, Calendar or document-viewer use may be processed in the countries where those global providers operate.
OpenStreetMap geocoding	Typed address queries, IP address and request metadata are sent to the configured OpenStreetMap-based geocoding provider. Its operator and hosting location must be confirmed in the App's production configuration.
Service NSW and Dribl	The Service NSW connection is currently sandbox-only. The App retrieves public Dribl fixtures and results read-only and does not send Club personal information for that retrieval.

Provider locations and subprocessors can change. Where the APPs apply, the Club will take reasonable steps appropriate to the service, such as minimising transferred data, selecting an Australian or privacy-protective region where reasonably available, restricting access, reviewing provider terms and updating this country list when a material change is identified. Overseas privacy protections may differ from Australian law.

13. When we disclose personal information

The Club may disclose only the information reasonably needed to:

- Provide authentication, database, cloud storage, backend, forms, email, notifications, payments, shop, sandbox voucher testing, ticketing, address search, public fixture and technical-support functions through the providers described in this policy.
- Manage football registration, competition, insurance, integrity, child safety and disciplinary processes with Football Australia, Football NSW, BDSFA, PlayFootball, Dribl or another authorised football body.
- Complete a transaction or communication requested by the user with Square, Jotform, Brevo or the configured Service NSW sandbox.
- Upload an event photograph, sponsor logo or gear image deliberately selected by an authorised committee or admin user to Firebase Cloud Storage.
- Send typed event-address text to the configured OpenStreetMap-based geocoding service for autocomplete suggestions.
- Prepare an authorised export for a role such as Registrar, Secretary or Treasurer where needed for Club administration and kept secure by the recipient.
- Respond to an emergency, serious safeguarding concern, suspected child abuse or threat to life, health or safety, including disclosure to emergency services, police, child-protection authorities or an authorised welfare contact.
- Obtain professional advice, insurance support, audit or technical assistance subject to appropriate confidentiality.
- Comply with a law, warrant, subpoena, court order, regulator request or other lawful requirement.
- Transfer App operations or systems to a replacement provider or Club administrator who must continue to protect the information and use it only for an authorised purpose.

The Club does not sell or rent personal information. Sponsor logos and acknowledgements are general Club content. The Club will not provide a sponsor with a member contact list for direct marketing without specific permission or another valid legal basis.

14. How we protect information

The Club takes reasonable technical, organisational and administrative steps proportionate to the sensitivity of the information and the risk to children, families and volunteers.

- Firebase Authentication and authenticated sessions for private functions.
- Firestore security rules and backend permission checks based on user, family, team, conversation and committee role.
- Private defaults for child, address, emergency-contact, payment, WWCC, complaint and committee-contact information.
- No normal under-18 accounts; restricted junior view-only access has no chat, purchasing, RSVP or shop features, and availability changes require parent approval.
- Six-digit parent-linking verification and parent-controlled junior player and referee records.
- Server-side service credentials and API keys rather than secrets embedded in the mobile App.
- Encrypted network connections and provider encryption at rest where supported.
- Committee permissions limited by duty, MPIO/CSO-only complaint and WWCC access, and removal of access when duties end.
- FFA numbers sent only to the registered email address and not displayed in the App.
- Provider review, software updates, proportionate security logs, backups and incident escalation.
- Committee confidentiality, child-safe handling, media-consent processes and restricted Firebase Storage uploads.
- Minimisation of notification previews even though an operational payload may contain a player name or payment amount.
- No analytics, advertising or tracking SDKs.

Users also protect the account

Use a strong unique password, protect the device, keep the App updated, do not share a linking code, check locked-screen notification settings and notify the Club promptly if an account or registered email may be compromised.

No internet, email or storage system is completely secure. Security controls reduce risk but cannot guarantee that an incident will never occur.

15. Retention, account deletion and de-identification

The Club keeps information only for as long as reasonably needed for the purposes in this policy, to protect participants and the Club, resolve disputes, maintain financial or association records and comply with law.

Record	Retention approach
Account and profile	While active and until deletion is completed, subject to records that must be kept. Inactive data is periodically reviewed.
Player, family and team	While needed for registration and participation, then deleted, de-identified or retained only as a necessary Club, football or legal record.
Goals, awards, attendance and lineups	For the season and Club record period needed for participation, recognition, disputes or historical reporting, then deleted or de-identified when no longer needed.
Messages	For the life of the relevant conversation or team need, and longer only for a safety report, complaint, dispute, legal requirement or conversation integrity.
Complaints and child-safety	For as long as reasonably needed to investigate, protect participants, document the outcome and meet legal, insurance or governing-body requirements.
Referee application and program	While the application is assessed and the referee participates, plus any period needed for fee, safeguarding, dispute or Club records.
WWCC	While the person holds a child-related role and for a reasonable compliance or audit period, then securely deleted or de-identified.
Payment and transaction	For tax, finance, association, audit and fraud-prevention obligations, commonly at least 5 to 7 years. This may include Square references, buyer details, player payment notes, card brand, last four digits and expiry, not full card details.
Voucher code	Not retained by the App. The current sandbox may keep technical test logs under its own settings. If live redemption is enabled, the retention wording and collection notice must be reviewed.
Uploaded media	While needed for the event, sponsor arrangement or shop listing and while any required media consent remains valid, then deleted or archived under an authorised Club record process.
Technical and security logs	Only as long as needed for security, troubleshooting and reliable delivery, and longer when linked to an incident or lawful requirement.
Backups and device cache	Deleted data may remain temporarily in protected backups until the ordinary backup cycle expires. An authorised offline cache, session, cart, saved-card reference or notification read state may remain locally until logout, clearing, deletion or uninstall.
Independent services	Square, Jotform, Brevo, Expo, map, geocoding, insurance and platform providers keep their own records under their notices and legal obligations.

Deleting an account

A user can start account deletion inside the App. The Club may verify identity before completing the request. Deletion removes or de-identifies the account and associated information from active Club systems except information required for a legal, financial, child-safety, fraud-prevention, complaint or dispute purpose. The Club aims to complete active-system deletion within 30 days, with protected backups expiring through the ordinary backup cycle.

Deleting an adult's account may unlink child players or junior referees and stop access to team functions. Content already shared with conversation participants may be retained when needed for safety, a complaint or conversation integrity, and otherwise deleted or de-identified where reasonably practicable. Deleting the App from a device does not by itself delete the account.

16. Access, correction and privacy choices

Subject to identity verification and lawful exceptions, a person may:

- View and update available account information in the App.
- Request access to information the Club holds about them or a child they are authorised to represent.
- Ask for inaccurate, out-of-date, incomplete, irrelevant or misleading information to be corrected.

- Ask for a family link, role, WWCC status, payment status or team assignment to be reviewed.
- Withdraw an optional consent, such as event-photo use or promotional email, without affecting earlier lawful handling.
- Turn off push notifications, camera, photo-library or calendar permission through device settings.
- Request deletion or de-identification of information no longer needed and use in-App account deletion.
- Complain about how information has been handled.

Requests can be made in the App where a function exists or by emailing mjsc@outlook.com.au. The Club may request enough information to verify identity and authority, especially for a child. It aims to acknowledge requests promptly and respond within 30 days where practicable. If access or correction is refused, the Club will explain why where legally permitted and identify available complaint options.

17. Notifications and Club communications

The App may send push alerts for announcements, fixture changes, fee reminders and auto-debit receipts, as well as account-security, team, availability, ground-closure, referee and event notices. Brevo may send fee reminders containing player names and amounts owing, password-recovery messages, family-linking codes and FFA reminders from mjsc@outlook.com.au. Some communications are necessary to provide the App or manage participation.

The push token is saved against the person's account in Firestore. Expo and the device platform process the token, delivery information and notification payload, which may contain a player name or payment amount. Brevo processes the recipient name, email and message content. A push notification may appear on a locked screen and an email can be forwarded or accessed through a compromised inbox, so users should review preview settings. Users can control push permission and unsubscribe from optional promotional email, but turning off notices may mean missing time-sensitive Club information.

18. Data incidents and breach response

If the Club suspects that information has been lost, accessed or disclosed without authorisation, it will take reasonable steps to contain the incident, protect affected accounts, preserve evidence, assess likely harm and reduce recurrence. It may work with Firebase, Cloudflare, Square, Jotform, Brevo, Expo or another relevant provider.

Where the Notifiable Data Breaches scheme applies and an incident is likely to result in serious harm that cannot be prevented through remedial action, the Club will notify affected individuals and the Office of the Australian Information Commissioner as required. The Club may also notify people when formal notification is not required but notice would help them protect themselves.

Report a concern quickly

Secure the affected account or device and email mjsc@outlook.com.au with enough detail for investigation. Do not send a password, full card number, card security code or voucher code by email.

19. Privacy enquiries and complaints

A privacy enquiry, access or correction request, deletion issue or complaint can be sent to mjsc@outlook.com.au. Describe the issue, the account or person involved, the requested outcome and a safe contact method, but do not include more personal information than necessary.

Complaints made through the dedicated App complaint function are visible only to the MPIO and CSO. A person may choose the anonymous option, in which case the complaint record does not require the complainant's name. The complaint text itself may still identify a person, and providers may retain limited technical or security logs. The Club may be unable to provide a personal response or investigate fully if no safe contact method is supplied.

The Club will verify identity where needed, investigate fairly and aim to respond within 30 days where practicable. If a person is not satisfied and the Privacy Act applies, they may be able to complain to the Office of the Australian Information Commissioner at oaic.gov.au/privacy/privacy-complaints. Other complaint or safeguarding options may be available through NSW authorities, Football Australia, Football NSW or the competition body.

20. Third-party links and independent services

The App may open a website, government service, form, payment interface, football platform, map or app-store page operated by another organisation. That organisation's privacy notice applies when it collects information directly. The Club does not control an independent service after a person leaves the App or submits information to that service.

Where the Club embeds or connects a service, it seeks to transfer only the information reasonably needed for the requested function. Provider services, privacy terms, subprocessors and locations can change independently. Appendix A contains the provider links current at the effective date.

Destination	What happens
Square checkout and receipts	Opens Square pages or forms. Square directly receives buyer and card information; the App receives only limited payment results and references.
Jotform referee application	Information entered goes directly to Jotform. The required application record is then stored in Firebase for authorised referee administration.
Gow-Gates / ClaimsGateway	Opens the football-insurance claims portal. Claim information, which may include health or other sensitive details, is entered directly with the portal and is not received by the App unless the person separately gives it to the Club.
Apple Maps / Google Maps	Opens directions to fixed grounds, events or sponsors. The App does not send live GPS location, but the selected maps app may use device location if the user permits it.
Sponsor, email and phone links	Opens a sponsor website or the device's mail or phone app. The destination receives information the user chooses to send and may receive ordinary connection metadata.
Club PDFs	Policies and regulations open in an in-App browser. On Android a PDF may render through Google's document viewer, which can receive the document URL and ordinary request metadata.
Google Calendar on the web	Opens Google Calendar with the selected Club event details when the user chooses add-to-calendar.
OpenStreetMap address search	Typed event-address text is sent for autocomplete. Use a venue or business address, not a private home address or confidential text. Public Nominatim does not permit client-side autocomplete, so production must use a compliant hosted or third-party geocoder.
SMS composer	Pre-fills the lighting-controller number and text. Nothing is sent until the user presses send; the mobile carrier and recipient then process the message.

Opening an independent site or app can disclose ordinary connection information such as IP address, browser or device details, request time and referring page. Users should review the destination's privacy notice before entering personal, payment, location, health or claim information.

21. Changes to this policy and contact

The Club may update this policy when App features, providers, Club practices or law change. The current version will be available in the App and on the Club website. A material change to collection, use or disclosure will be notified in the App, by email or through another reasonable channel before or when it takes effect.

The policy will be reviewed at least annually and earlier after a material security incident, significant integration change, a new sensitive-data function or the registration of the Australian Children's Online Privacy Code.

Privacy contact

Minchinbury Jets Soccer Club Incorporated
 ABN 95 372 250 224
 Minchinbury Oval, 22 Minchin Drive, Minchinbury NSW 2770
 Email: mjsc@outlook.com.au
 Website: www.minchinburyjets.com

A. Main service providers

This table describes the principal services expected to support the App. The provider's current notice applies to information it processes directly. The Club should review this table whenever an integration or data region changes.

Provider	App function, data and location	Privacy information
Google Firebase	The minchinbury-jets-soccer-club project provides Authentication, Firestore and Cloud Storage. It holds accounts, players and children, registrations, teams, fixtures, lineups, chats, committee data, events, tickets, payments, WWCC, complaints, referee records, push tokens and uploaded event, sponsor and gear images. Authentication is US-only; database and storage depend on configured regions; Google may process globally.	Firebase privacy and security
Cloudflare	Backend and API services for payment plans (buyer name and email, player name, saved-card reference, brand and last four digits), shop refund requests and game-day duty rosters, plus IP and security logs. Primarily US and EEA storage, with global transfer or access.	Cloudflare privacy
Square	Square pages, forms and vault handle all card payments. Square receives buyer name and email and a player name in payment notes. The App keeps only references, brand, last four digits, expiry, results and receipts, not full card details. Identified processing countries include US, Canada, Japan, Ireland, France, Spain and UK.	Square buyer privacy

Provider	App function, data and location	Privacy information
Brevo	Club emails from mjsc@outlook.com.au, including fee reminders with player names and amounts owing, password recovery, linking codes and FFA reminders. Receives recipient name, registered email and message content. Main database hosting is stated in France, Germany and Belgium, with other subprocessors possible.	Brevo privacy Brevo storage locations
Jotform	The referee application opens Jotform, and data entered goes directly to Jotform, including applicant, under-18 and parent details. The required application record is then stored in Firebase for authorised Club users. Standard Jotform data is stored in the US unless another available region is selected.	Jotform privacy
Service NSW sandbox	The current Active and Creative Kids integration is test-only. The configured sandbox receives voucher code, child's name and date of birth and returns a test result. The App does not retain the code. Live redemption requires a policy and collection-notice review before launch.	Voucher privacy notice
Expo	Push delivery for announcements, fixture changes, fee reminders and auto-debit receipts. Receives push token and payload, which may contain a player name or payment amount, and may process end-user information in the US.	Expo privacy
Apple and Google	App distribution and push delivery, plus user-directed Apple or Google Maps, Google Calendar and Android Google document-viewer use. May process token, event, route, document URL, device, location (if the user permits it in Maps) and connection data under platform settings.	Apple Maps privacy Google privacy
OpenStreetMap geocoding	Receives typed event-address text and ordinary request metadata for autocomplete. The production operator and hosting location must be documented. Public Nominatim prohibits client-side autocomplete; production must use a compliant hosted or third-party service.	OSMF privacy Nominatim use policy
Gow-Gates / ClaimsGateway	User-directed football-insurance claim portal. Claim and possible health information is entered directly with the portal and is not collected by the App unless separately provided to the Club.	Gow-Gates privacy ClaimsGateway privacy
Dribl	Read-only retrieval of public fixtures, results, tables and match information. The Club sends no personal information to Dribl for that retrieval. Direct interaction is governed by Dribl's notice.	Dribl privacy
PlayFootball / Football Australia	Source of authorised participant and registration reports imported by the Club. No continuing App transfer is described in this policy; the source platform handles its own account data.	Football Australia privacy

B. Legal and guidance references

These official links informed the policy and are included for transparency. They do not replace legal advice about the Club's particular circumstances or technical implementation.

Topic	Official source
Australian Privacy Principles	OAIC - Australian Privacy Principles
APP privacy-policy requirements	OAIC - APP 1 guidance
Overseas recipients	OAIC - APP 8 guidance
Security and deletion	OAIC - APP 11 guidance
Notifiable Data Breaches	OAIC - NDB scheme
Children and young people	OAIC - children and young people
Children's Online Privacy Code	OAIC - Code status and milestones
Service NSW voucher collection	Service NSW - voucher notice
OpenStreetMap geocoding	OSMF - Nominatim use policy
Football insurance portals	Gow-Gates privacy ClaimsGateway privacy
Club legal entity	Australian Business Register - ABN 95 372 250 224

Implementation check

Before public release, confirm the Firebase regions, the production OpenStreetMap geocoder and its privacy notice, and whether Service NSW remains sandbox-only. This policy must be updated if the live App changes fields, access, analytics, location, providers or retention. Legal review is recommended.