CueCrew GDPR and Security Statement

Purpose and scope

This statement sets out how CueCrew protects personal data under UK GDPR and the Data Protection Act 2018, and lists the security settings the site must keep switched on to meet Article 32 (security of processing).

- **Covers:** the CueCrew platform at cuecrew.co.uk, every league site on it (for example wbppl.cuecrew.co.uk), its email and its server.
- **Controller:** CueCrew, a personal, not-for-profit project run by an individual (not a registered business), for accounts and the platform. The leagues on it are volunteer-run, not-for-profit clubs. League admins decide what goes on their own league's pages and must follow this statement.
- **Contact:** admin@cuecrew.co.uk.
- **Public notice:** the privacy notice people see is at cuecrew.co.uk/privacy. This statement is the internal record behind it.

This was written alongside the site build and is not legal advice; have it reviewed before relying on it.

Personal data we hold

CueCrew holds the minimum needed to run leagues: no payment details, no special-category data, no tracking or advertising data.

Data	Whose	Why	Lawful basis
Name, email, password hash	Account holders	Sign-in and account emails	Contract (providing the service)

Data	Whose	Why	Lawful basis
Player name, team, frames played and results	Players, with or without an account	Running the league: fixtures, tables, stats	Legitimate interests (the league and its players)
Player email and phone (optional)	Players, added by admins or captains	Arranging matches	Legitimate interests
Bug reports, comments, join and claim requests	Account holders	Support and league membership	Contract
Sign-in records: sessions with a device description (e.g. Safari on iPhone), trusted devices, failed-login counts (against a scrambled email), sign-in codes, and a public key per device for Face ID / fingerprint sign-in	Account holders	Security	Legitimate interests and legal obligation (Article 32)
Audit log of changes by admins and captains	Account holders	Tracing and correcting mistakes	Legitimate interests

Security settings

These settings are CueCrew's technical measures under Article 32 and must stay on. Two can be switched off by a super admin (Super admin → Leagues); turn them off only briefly, for example while email delivery is being fixed, and note when and why.

Area	Setting	Value	Can be switched off?
Sign-in	Lockout after wrong passwords	5 wrong attempts locks sign-in for 15 minutes; the owner is emailed; counted per email address so it can't reveal who has an account	No

Area	Setting	Value	Can be switched off?
Sign-in	Emailed sign-in code (two-step)	6-digit code, valid 10 minutes, 5 tries, new code after 1 minute, at most 5 per sign-in	Yes: *Emailed sign-in codes*
Sign-in	Who needs a code	Super admins every sign-in; everyone else only the first time on a new device or browser (the device is then remembered for 90 days). Face ID / fingerprint can be used instead of the code	No
Sign-in	Face ID / fingerprint (passkeys)	Optional, set up per device; the face or fingerprint never leaves the device and CueCrew stores only a public key; counts as both sign-in steps; removable on the account page	No (people choose whether to use it)
Sign-in	New accounts confirm their email	A link valid 48 hours; password needed to confirm	Yes: *People who register must confirm their email*
Sessions	Confirm it's you before sensitive pages	Pages and actions that reach other people's contact details (all Admin pages, a team's Manage tab, the bug list) and Download my data / Delete my account need Face ID / fingerprint or an emailed code within the last 4 hours	No
Sessions	Maximum session length	90 days; 1 day when a super admin impersonates. Every signed-in device is listed on the account page and can be signed out	No
Sessions	Unattended live pages	Live-score refresh pauses after 10 minutes without use, so a screen nobody is looking at stops loading	No

Area	Setting	Value	Can be switched off?
Passwords	Storage	One-way bcrypt hash (cost 12); never stored or emailed in plain text	No
Passwords	Minimum length	8 characters	No
Passwords	Reset	Emailed link, single use, valid 1 hour, newest only, 1 per minute; the same message whether or not the email exists	No
Passwords	After a change	Signs out every other device and forgets trusted devices	No
Connection	Encryption in transit	HTTPS only, Let's Encrypt certificates behind the Nginx proxy	No
Connection	Cookies	Essential only: session, sign-in code, trusted device (90 days) and a 5-minute Face ID / fingerprint check; all HttpOnly and Secure	No
Server	Database	PostgreSQL on an internal Docker network; never published to the internet	No
Email	Sending	Microsoft 365 via an app that can send only as noreply@cuecrew.co.uk (Exchange RBAC); SPF, DKIM and DMARC set	No
Links	Single-use tokens	Reset, confirm and invite links are stored only as hashes and can't be used twice	No
Server	Backups	Nightly and pre-update database backups encrypted with a public key (GPG, RSA 4096); the private key and passphrase are kept off the server; backup folder readable by root only	No

Area	Setting	Value	Can be switched off?
Contact details	Permission check	Admins and captains must confirm they have the person's permission, and the details are needed, before adding or changing an email or phone number or sending an invite; the server refuses the save otherwise; bulk imports need a tick	No

Why sign-in works this way

Sign-in checks are matched to how much personal data each role can reach, as Article 32 asks for security appropriate to the risk. This section is the record of that decision, made on 3 November 2026.

Role	Other people's personal data they can reach	Checks
Player	None (their own account and public league pages)	Password; emailed code on a new device; signed in up to 90 days; Face ID / fingerprint optional
Captain / vice captain	Their team's emails and phone numbers (Manage tab)	As a player, plus a check within the last 4 hours before the Manage tab or any roster change
League admin	Every contact detail in their league	As a player, plus a check within the last 4 hours before any Admin page or admin action
Super admin	Everything on the platform	Code or Face ID / fingerprint at every sign-in, plus the 4-hour check

The personal data CueCrew holds is limited to names, contact details and match results, with no special-category or financial data. A long session is therefore proportionate, because nothing that shows other people's contact details opens without a recent check. Face ID / fingerprint is stronger than an emailed code and can't be phished.

The previous settings (a code every sign-in for admins, daily for everyone else, and sign-out after 1–3 hours idle) were replaced after members reported that daily codes and mid-evening sign-outs got in the way of using the site, with no matching gain in protection for the data involved. Review this choice with the rest of the statement.

Access control and accountability

Each role sees and changes only what it needs, and every change is recorded.

Role	Can see	Can change	How it's granted
Public	League pages: fixtures, results, tables, player names and stats	Nothing	No account
Player	As public, plus their own account and data	Their account and availability	Registers, or joins by invite
Captain / vice captain	Their team's roster and the contact details the league holds	Their team's lineups, results, invites	Set by a league admin
League admin	Everything in their league	Everything in their league	Added by another admin of that league
Super tester	The bug and idea list	Bug reports	Granted by a super admin
Super admin	Everything on the platform	Everything; can impersonate a user for support	Only from the server (`npm run create-superadmin`)

- **Audit log:** every change by an admin or captain (results, rosters, settings, uploads) is logged with who, when, and before and after.
- **Impersonation log:** each time a super admin signs in as someone else is logged, and a banner shows throughout.
- **Lifetime bans:** checked whenever someone registers, joins or is added to a team.

People's rights

People can use most of their rights themselves on the site; the rest come to admin@cuecrew.co.uk and must be answered within one month.

Right	How it works
Be informed	Privacy notice at /privacy, linked from every page footer, the sign-in pages and the registration form. Everyone signed in sees a short summary pop-up once, and again only when the notice changes
Access	My account → *Download my data*: account, player records, every frame played, notifications, requests, reports, sign-ins (JSON)
Rectification	Account details on My account; league records corrected by the league admin
Erasure	My account → *Delete my account* (password and typing DELETE). Removes the login, notifications, requests and devices. Match results stay, because other teams' results depend on them; the person can choose to have their name replaced with "Former player". The only admin of a league must add another admin first
Object or restrict	By email; a league admin can remove a player's contact details or the player record

How long we keep data

Data is kept only as long as it's needed.

Data	Kept for
Account	Until the person deletes it
League results and player records	As long as the league keeps its history
Sessions	Until sign-out, or 90 days
Sign-in codes	10 minutes
Trusted devices	90 days
Face ID / fingerprint keys	Until removed on the account page, or the account is deleted
"Confirmed it's you" for sensitive pages	4 hours
Password reset links	1 hour

Data	Kept for
Email confirmation links	48 hours
Team invites	14 days
Uploaded spreadsheets waiting for confirmation	Deleted when imported, or after 1 day
Nightly database backups	7 days (one per weekday, overwritten)
Backups taken before each update	The 10 most recent
Audit and impersonation logs	2 years, then deleted automatically (checked at start-up and once a day)

Hosting and processors

CueCrew runs on its own server in the UK. One outside company handles personal data for us.

Who	What they do	Data they see	Safeguard
Microsoft 365	Sends CueCrew's emails (codes, resets, invites, notices) and hosts the cuecrew.co.uk mailboxes	Recipient name and email, message text	Microsoft's data processing terms (part of the 365 subscription)
CueCrew server (UK, self-hosted, behind a WatchGuard firewall)	Runs the site and database	Everything	Firewall; database not exposed; HTTPS only
Let's Encrypt	Issues the HTTPS certificate	None (domain names only)	Not a processor

The Microsoft 365 app secret expires in **October 2028** and must be renewed before then.

Still to do

The site's technical measures are in place; these organisational steps are not yet done.

- [ ] Check whether CueCrew must pay the ICO data protection fee (ico.org.uk self-assessment; usually £40–60 a year for a small organisation) and register if so
- [ ] Have the privacy notice and this statement reviewed by someone qualified
- [ ] Write a one-page breach plan: who decides, how to contain it, and reporting serious breaches to the ICO within 72 hours
- [ ] Run deploy/setup-backup-key.sh once to encrypt backups, store the private key and passphrase off the server, and limit who can sign in to the server
- [ ] Keep the server, Docker images and Node packages patched (at least monthly)
- [ ] Renew the Spamhaus listing removal if it's ever needed again (it lasts a year) and the Microsoft 365 app secret by October 2028

Review

Review this statement every 12 months, and whenever the site starts collecting new kinds of data or a security setting changes.

Version	Date	Change	Approved by
1.0	21 October 2026	First version, written alongside the site's security update	
1.1	3 November 2026	Sign-in matched to risk: 90-day sessions, code only on new devices, Face ID / fingerprint, a 4-hour check before contact details and admin pages (site version 1.3.0)	