

Old Wilsonians Football Club UK GDPR Data Protection Policy — February 2026

This policy sets out how Old Wilsonians Football Club complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and how we protect personal data of members, players, parents/carers, volunteers and officials.

Data Protection Lead	Jamie Parkinson, Club Secretary
Contact	Use the contact details published on the club website or write to the Club Secretary at the clubhouse address.

1) Scope & Definitions

This policy applies to all personal data processed by OWFC in connection with football activities, including youth and open■age teams, administration, events and digital platforms (website, email, messaging apps, league systems). It covers players (including U18s), parents/carers, referees, volunteers, committee members, coaches, and spectators where applicable.

2) Our Lawful Bases for Processing

We rely on the following lawful bases under Article 6 UK GDPR: consent; contract; legal obligation; legitimate interests. Where we process special category data (e.g., medical info), we rely on Article 9(2)(a) explicit consent or 9(2)(c) vital interests, and for safeguarding/DBS records, relevant Schedule 1 conditions under the DPA 2018, with appropriate policy documentation.

3) What Data We Collect

- Identity & contact (name, DOB, address, email, phone; parent/carer for U18s).
- Registration & eligibility (club/league/FA numbers, team allocations, kit sizes).
- Medical & accessibility (allergies, injury info, access needs).
- Safeguarding & conduct (incident logs, referrals, low■level concerns, sanctions).
- DBS status (pass/expiry). We do not retain full certificate details or conviction data beyond what is lawful and necessary.
- Images & media (team photos, match footage) subject to consent and club annex rules.
- Systems metadata (Club Portal roles, course completions, attendance registers).

4) How We Use Personal Data

- Register players and volunteers; run teams, fixtures, and events; provide communications about football activity.
- Safeguarding: keep children and adults at risk safe; maintain incident logs and reporting to The FA/County FA and statutory agencies where appropriate.
- Compliance: affiliation, insurance, audit and disciplinary matters.
- Development: training records for CWOs, coaches and committee; accreditation evidence.

5) Who We Share Data With

- The FA / County FA / leagues and competition organisers (affiliation, fixtures, Whole Game / Club Portal).
- DBS provider (First Advantage) for criminal records checks of eligible roles.
- Medical professionals and emergency services where necessary to protect life.
- Police, Local Authority children's/adult safeguarding where required by law or to protect individuals.
- Accredited IT/service providers used by the club (e.g., email, cloud storage) under written data processing terms.

6) Children's Data & Parental Consent

For U18s we prioritise safety and privacy. We obtain parental/carers consent where required; avoid publishing identifying details with images; and apply "no 1 to 1 messaging" rules for digital comms. We implement proportionate age appropriate information for young people about how their data is used.

7) Photography & Media

We follow club photography/filming rules (consent registers, no changing area images, commissioning controls). Where consent is refused or withdrawn we will avoid taking or remove images involving that individual from club channels where feasible.

8) Retention Schedule (Summary)

Data Category	Typical Retention
Player/member records	Up to 2 years after membership ends (financial records 6 years).
Safeguarding/disciplinary case files	Up to 75 years, in line with FA safeguarding guidance and legal limitation period
DBS status logs	Length of role + up to 3 years (do not store full certificate details).
Accident/incident reports (non safeguarding)	7 years (or longer for serious injury claims).
Images & media	Until consent withdrawn or the stated purpose ends; reviewed annually.

We hold detailed retention notes internally and will provide them on request.

9) Security Measures

- Role based access control; least privilege; regular access reviews.
- Strong authentication; device encryption; secure cloud storage; regular backups.
- Data processing agreements with third party providers; UK hosting or UK adequate transfer safeguards.
- Staff/volunteer training on handling children's data and safeguarding records.

10) International Data Transfers

We seek to store/process personal data in the UK. If we use services that transfer data outside the UK, we will ensure an adequacy decision or appropriate safeguards (e.g., IDTA/standard clauses) are in place.

11) Your Rights

- Right to be informed; access; rectification; erasure; restriction; portability; object; and rights in relation to automated decision making.
- To exercise your rights, contact the Club Secretary (Data Protection Lead). We will respond within one month unless an extension is lawful.

12) Subject Access Requests (SARs)

Please describe the information sought and the context (e.g., role, season). We will verify identity (and parental responsibility for U18s) before releasing data. Where requests involve third-party data we will redact or seek consent where appropriate.

13) Data Breach Response

- Contain and assess: stop the breach; secure systems; start an incident log.
- Evaluate risk to individuals (especially U18s) and decide if the ICO and/or data subjects need to be notified within 72 hours of awareness.
- Implement remedial actions and lessons learned; update policies and training as needed.

14) Complaints & ICO

If you have concerns, contact the Club Secretary first. You also have the right to complain to the Information Commissioner's Office (ICO). See ico.org.uk for current contact details.

15) Related Club Policies

- Safeguarding Policy (Children & Adults at Risk) and Annexes (Digital, Photography, Changing Rooms, Trips/Transport/Ratios).
- Codes of Conduct; Equality, Anti-Discrimination; Complaints/Discipline.

16) Review Cycle

This policy is approved by the Committee and reviewed annually (or sooner after a significant incident, service change, or legal update). Current edition: February 2026.

Document control: This PDF is web■optimised for publication on the OWFC website.