



Middlesbrough RUFC - GDPR Policy

1 Purpose

This policy sets out how Middlesbrough Rugby Union Football Club (“the Club”) manages, processes, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It applies to all Club officials, committee members, coaches, volunteers and anyone who handles personal data on behalf of the Club.

2 Scope

This policy covers all personal data processed by MRUFC, whether in digital or paper form, relating to:

- Current and former players (senior, junior, and minis)
- Parents and guardians of junior/minis players
- Volunteers, coaches, referees, committee members and staff
- Suppliers, sponsors and partners
- Visitors and event participants

Data may be processed via the RFU Game Management System (GMS), Pitchero, Spond, email, spreadsheets or other approved Club systems.

3 Definitions

- Personal Data: Information identifying an individual, directly or indirectly.
- Special Category Data: Sensitive data (e.g. medical, safeguarding, ethnicity).
- Processing: Any action performed on data (collection, storage, sharing, deletion).
- Data Controller: MRUFC (the legal entity).
- Data Processor: Any external service processing data on behalf of MRUFC.

4 Data Protection Principles

MRUFC processes personal data in line with the following principles:

- Lawfulness, fairness and transparency
- Purpose limitation - used only for legitimate Club purposes
- Data minimisation - only data necessary for purpose is collected
- Accuracy - kept up to date and corrected where necessary
- Storage limitation - retained only as long as necessary
- Integrity and confidentiality - secured against unauthorised access
- Accountability - the Club must demonstrate compliance

5 Lawful Bases for Processing

MRUFC processes personal data under one or more of the following lawful bases:

- Contract - to manage player membership and participation
- Legal obligation - to meet statutory or RFU requirements
- Legitimate interests - to operate and promote the Club safely and effectively
- Consent - for communications, photos and optional activities
- Vital interests - where necessary for medical or safeguarding purposes

6 Key Roles and Responsibilities

- Club Committee - overall accountability for compliance.
- Data Protection Officer - oversees data handling practices and compliance with this policy.
- Safeguarding Officer - manages safeguarding data, disclosures and restricted access.
- All officials and volunteers – must follow this policy when handling data.



7 Data Storage and Security

Personal data must be stored securely and only accessible to authorised persons. Approved Club systems:

- RFU GMS - membership and player registration
- Pitchero and Spond - team management and communication
- Email and spreadsheets - administrative records (restricted use)

Data should not be shared using unencrypted personal email accounts or unauthorised file-sharing platforms.

Note: Gmail accounts used by the Club provide encryption in transit (TLS) and are compliant with UK GDPR when properly secured. Users must ensure their accounts are password-protected, used only for Club purposes and access is limited to authorised individuals.

8 Use of Personal Devices and Communications

Personal devices (such as phones, laptops or tablets) may be used for Club purposes under the following conditions:

- Club-related data should be processed or stored on personal devices only where necessary.
- Devices must be protected by passwords or PINs and data should be stored securely.
- Club data remains the property of MRUFC regardless of the device used.
- Personal data on private devices unrelated to Club activity is outside the Club's jurisdiction.
- Users must delete or securely transfer Club data when they cease their role.
- Messaging apps (WhatsApp, SMS, Messenger) should be used only for essential operational communication and not for sensitive or disciplinary matters.
- The Club has no obligation or authority to search personal devices for data but individuals are expected to cooperate with lawful data access requests if they have processed Club data on personal systems.

9 Data Sharing

Data may only be shared:

- Within the Club, on a "need to know" basis
- With the RFU or affiliated bodies for regulatory or disciplinary purposes
- With safeguarding or statutory agencies where required by law or welfare concerns
- With third-party processors who meet GDPR compliance standards

Personal data will never be sold or shared for marketing purposes outside the Club.

The Club uses trusted third-party platforms such as the RFU's GMS, Spond and Pitchero to manage membership and communications. These platforms process data on behalf of the Club under data-processing agreements that comply with UK GDPR. Each platform operates its own independent privacy policy and may seek members' separate consent to receive marketing or promotional materials directly from them. Where this occurs, it is the platform (not the Club) acting as the Data Controller for that specific purpose.

10 Retention and Deletion

Data will be retained in line with the Club's retention schedule, typically:

- Membership and participation records: up to 6 years after last activity
- Safeguarding and disciplinary records: minimum 7 years, longer if required
- Financial records: 7 years for HMRC purposes

Data must be deleted or anonymised when no longer required.



11 Children, Juniors and Minis

For players under 18:

- Data will be processed with parental or guardian consent.
- Safeguarding and welfare information is restricted to relevant officers.
- Photos, videos or media use must comply with the Club's Safeguarding Policy.

12 Subject Access Requests (SARs)

Individuals have the right to access their personal data. Requests must be made in writing to the Club Secretary or Safeguarding Officer.

- The Club must respond within one calendar month.
- If the request is complex, the Club may extend by up to two further months with notice.
- If the request is manifestly unfounded or excessive, the Club may refuse or charge a reasonable administrative fee but must justify the decision.
- The Club is not required to obtain or disclose data from personal devices or accounts outside its control systems.

13 Data Breach Management

Any data loss, unauthorised disclosure or suspected breach must be reported immediately to the Data Protection Lead and Safeguarding Officer (if minors are involved). Serious breaches will be notified to the ICO and affected individuals within 72 hours where required.

14 Training and Awareness

All officials, coaches and volunteers handling personal data must:

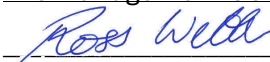
- Read and understand this policy
- Complete RFU or Club GDPR/safeguarding awareness training
- Report any concerns promptly

15 Review and Updates

This policy will be reviewed annually or following any material changes in data protection legislation, Club systems or safeguarding procedures.

Version: 1.0

Approved by: The Management Committee

Signed: 

Date: Wednesday, October 29, 2025

Next review: *(due 12 months from date of this document).*