

Staff Privacy Notice

1. Who We Are

Birmingham City Football Club Limited and Birmingham City Women Football Club Limited (“we”, “us”, “our”) process personal data relating to employees, workers, contractors, consultants, volunteers, apprentices, interns, agency workers, casual workers, and former members of staff.

This privacy notice explains how we collect, use, store, share, and protect personal data as part of managing the employment relationship, workforce administration, football operations, safeguarding, stadium operations, matchday activities, ticketing, accreditation, access management, information security, and wider business operations.

This notice applies across all areas of the Clubs, including:

- Men’s First Team
- Women’s First Team
- Boys’ Academy
- Girls’ Academy
- Football Operations
- Coaching, Medical, Sports Science and Performance Departments
- Recruitment and Talent Identification
- Stadium and Matchday Operations
- Corporate and Support Functions
- Community and Public-Facing Activities

We are committed to protecting personal data and ensuring compliance with UK GDPR and the Data Protection Act 2018.

Data Controllers: Birmingham City Football Club Limited and Birmingham City Women Football Club Limited

Address: St Andrew’s @ Knighthead Park, Cattell Road, Birmingham, England, B9 4RL

Data Protection Officer: dpo@bcfc.com

2. What Personal Data We Collect

We collect and process personal data as part of employment, workforce management, safeguarding, football operations, and the administration of the Clubs.

a. Identification & Contact Data

- Name
- Date of birth
- Gender
- Photograph
- Nationality
- Home address
- Telephone numbers
- Email addresses
- Emergency contact details

b. Employment & Workforce Data

- Employee number
- Job title and department
- Employment status
- Contract details
- Start date and leaving date
- Working hours and work patterns
- Employment history
- Performance and appraisal records
- Objectives and KPI records
- Promotion and role change information
- Succession planning information
- Disciplinary and grievance records
- Conduct and behavioural records

c. Payroll, Benefits & Financial Data

- Salary and remuneration information
- Bonus and incentive information
- Bank account details
- National Insurance number
- Tax information
- Pension information
- Benefits enrolment information

- Expenses and reimbursement records

d. Recruitment & Vetting Data

- CVs and application forms
- Qualifications and certifications
- Interview notes and assessment records
- References and referee details
- Right-to-work documentation
- DBS checks where required
- Safeguarding checks where required
- Recruitment agency information
- Pre-employment screening results

e. Learning, Development & Compliance Data

- Training records
- Professional qualifications
- Continuing Professional Development records
- Mandatory compliance training records
- Safeguarding training records
- Coaching licences and accreditations
- Regulatory or role-specific training records

f. Attendance & Workforce Management Data

- Holiday and absence records
- Sickness absence records
- Flexible working requests
- Shift and rota information
- Travel and accommodation information
- Driving Licence & insurance Details
- Vehicle, mileage, and parking information
- Asset allocation records, including laptops, phones, passes, and equipment

g. IT, Communications & System Usage Data

- User account details
- Login and access records
- Email metadata and communication logs
- Device identifiers
- IP Address

- Cookies
- System audit logs
- Network and cybersecurity monitoring records
- Information security investigation records
- Internet and system usage records

h. CCTV, Security & Access Management Data

- CCTV footage
- Access card records
- Visitor management logs
- Building and site access records
- Security incident reports
- Body-worn camera footage where used in security environments

i. Coaching, Performance & Workforce Analysis Data Where Applicable

For coaching, football, performance, analysis, and technical staff, we may process:

- Coaching session recordings
- Training and match analysis footage
- Coaching observations and assessments
- Performance reviews and evaluations
- Session planning and development records
- Professional qualifications and coaching licences
- KPI and objective tracking
- Technical and tactical analysis records
- Workforce planning and succession planning information

j. Ticketing, Accreditation & Access Data

- Staff ticket allocations
- Ticketing account information
- Single Sign-On (SSO) account information
- Authentication and identity verification data
- Ticketing account identifiers
- Matchday accreditation records
- Hospitality access records
- Event and matchday attendance records
- Stadium and training ground access permissions
- Access control and entry logs
- Vehicle permit and parking information

3. Special Category Data Where Relevant

Where necessary and lawful, we may process special category data and criminal offence data.

Health & Medical Data

- Occupational health records
- Disability information
- Workplace adjustment information
- Fit notes and medical certificates
- Health and wellbeing information
- Sickness absence information
- Injury or medical information relevant to employment, safeguarding, or health and safety

Equality, Diversity & Inclusion Data

Where voluntarily provided, this may include:

- Sex / gender
- Gender identity
- Ethnicity and racial or ethnic origin
- Disability
- Neurodiversity
- Religion or belief
- Sexual orientation
- Caring responsibilities
- Marital status
- Pregnancy and maternity information
- Socio-economic background

Education background

This information may be used to:

- Monitor equality, diversity, and inclusion
- Meet legal and regulatory obligations
- Promote fair employment practices
- Identify and address barriers to inclusion
- Support workforce reporting and inclusion initiatives

Where possible, EDI data is used in aggregated or anonymised form.

Safeguarding Data

Where relevant to a role, incident, or safeguarding matter, we may process:

- DBS information
- Safeguarding training records
- Safeguarding concerns or referrals
- Welfare reports
- Investigation records
- Risk assessments
- Case management records

Criminal Conviction Data

We may process criminal offence data where required by law, safeguarding obligations, regulatory requirements, or where necessary for roles involving children, vulnerable individuals, financial responsibility, security, or positions of trust.

Trade Union Membership Data

We may process trade union membership information where required for employment purposes, legal obligations, or where voluntarily provided by the individual.

Special category data is processed with enhanced safeguards, including:

- Restricted access
- Role-based permissions
- Secure storage
- Data minimisation
- Enhanced confidentiality controls
- Separation from general employment records where appropriate

4. How We Use Your Data

We process personal data for the following purposes.

Recruitment & Onboarding

- Assess suitability for employment
- Verify qualifications and references
- Complete right-to-work checks
- Conduct DBS and safeguarding checks where required
- Complete employment contracts and onboarding processes

Employment Administration

- Manage contracts and employment relationships
- Maintain personnel records
- Manage working arrangements & duties
- Support internal communications
- Administer policies and procedures

Payroll, Pension & Benefits

- Process salary payments
- Administer pensions and benefits
- Process expenses and reimbursements
- Meet tax, HMRC, payroll, and pension obligations

Performance & Development

- Conduct appraisals and performance reviews
- Manage objectives and KPIs
- Deliver training and development
- Monitor professional qualifications
- Support promotion, progression, and succession planning

Learning, Development & Compliance

- Deliver mandatory and optional training
- Monitor training completion
- Ensure compliance with regulatory and safeguarding requirements
- Maintain professional development and accreditation records

Attendance & Workforce Management

- Manage absence and leave
- Monitor attendance

- Manage rotas, shifts, and staffing levels
- Support workforce planning and operational resourcing

Health, Safety & Welfare

- Protect staff welfare
- Meet health and safety obligations
- Provide occupational health support
- Manage workplace adjustments
- Record and investigate workplace accidents and incidents

Safeguarding

- Protect children, vulnerable individuals, staff, players, visitors, supporters, and members of the public
- Conduct safer recruitment checks
- Manage DBS and safeguarding requirements
- Investigate safeguarding concerns
- Maintain safeguarding records
- Meet statutory, FA, league, and regulatory safeguarding obligations

Coaching & Performance Analysis

Where applicable, we process personal data to:

- Review and improve coaching performance
- Evaluate training delivery and coaching effectiveness
- Support professional development and performance management
- Analyse coaching sessions, matches, and training activities
- Monitor compliance with coaching standards, football methodologies, operational procedures, and performance frameworks across Birmingham City Football Club Limited and Birmingham City Women Football Club Limited

Ticketing, Accreditation & Access Management

We process personal data to:

- Allocate staff tickets and matchday accreditation
- Provide access to stadium and training facilities
- Manage Single Sign-On (SSO) authentication and identity verification for ticketing, accreditation, access management, and connected systems
- Manage security and access permissions

- Monitor attendance at matches and events
- Manage hospitality, parking, and vehicle access
- Ensure the safety and security of staff, visitors, players, and facilities

Information Security & Business Operations

We process personal data to:

- Protect the systems, networks, facilities, information assets, and operations of Birmingham City Football Club Limited and Birmingham City Women Football Club Limited
- Manage and administer user accounts, permissions, role-based access controls, and identity management processes
- Operate and maintain Single Sign-On (SSO) authentication services across systems and platforms
- Verify user identities and manage authentication credentials
- Manage access to systems, applications, data, facilities, and operational resources
- Detect, investigate, and prevent cybersecurity incidents
- Monitor compliance with information security policies and procedures
- Detect unauthorised access, misuse of systems, or security threats
- Support audit, governance, and compliance activities
- Maintain business continuity and operational resilience
- Protect confidential, commercially sensitive, and personal information

CCTV & Security

We use CCTV, access control, and security systems to:

- Protect staff, players, visitors, supporters, and property
- Prevent and detect crime
- Investigate incidents
- Support safeguarding, health and safety, and public safety obligations
- Monitor access to facilities, training grounds, offices, stadium environments, and operational locations

Governance, Legal & Compliance

We process personal data to:

- Meet legal, regulatory, and employment obligations
- Respond to complaints, claims, audits, and investigations
- Maintain governance and accountability records

- Support reporting to regulators, auditors, governing bodies, and law enforcement where required

AI & Profiling

We may use AI tools and automated technologies to support:

- Recruitment administration and candidate screening
- Workforce analytics and reporting
- Data Analysis & Reporting
- Resource planning and operational management
- Information security monitoring and threat detection
- Policy compliance monitoring
- Learning and development analysis
- Coaching performance analysis and benchmarking
- Workforce and coaching development planning

For coaching, football, performance, and technical staff, AI and analytical tools may be used to:

- Review coaching session delivery and effectiveness
- Analyse training and match activities
- Assess coaching performance against objectives and KPIs
- Identify development opportunities and training needs
- Support performance reviews and professional development discussions
- Benchmark coaching practices and outcomes across departments
- Monitor compliance with coaching standards and methodologies

AI and analytical tools are used to support decision-making and provide insights. Significant employment decisions are not made solely by automated means.

Safeguards include:

- Human oversight and review
- No solely automated employment decisions with legal or similarly significant effects
- Ability to challenge decisions where applicable
- Regular review of outputs for accuracy, fairness, and relevance
- Proportionate and transparent use of AI and profiling technologies
- Appropriate governance, security, and accountability controls

5. Lawful Bases for Processing

We rely on a number of lawful bases under Article 6 UK GDPR depending on the nature of the processing activity being undertaken.

Article 6(1)(a) Consent

Where consent is required and can be freely given, including:

- Optional benefits and wellbeing initiatives
- Certain equality, diversity, and inclusion initiatives
- Optional photography, media, or promotional activities
- Other optional processing activities where consent is appropriate

Article 6(1)(b) Contract

Processing necessary to enter into, administer, and fulfil employment, worker, consultancy, volunteer, or other contractual arrangements, including:

- Recruitment and onboarding
- Employment administration
- Payroll and benefits administration
- Workforce management
- Performance management
- Coaching and performance management
- Learning and development
- Training and accreditation
- Workforce planning relating to role fulfilment
- Travel and accommodation arrangements
- Provision of equipment, systems, and facilities
- Ticketing and accreditation required for employment duties
- Role-based access management
- Single Sign-On (SSO) authentication required to access employment systems
- Football operations directly connected to an individual's role
- Matchday duties and operational responsibilities

Article 6(1)(c) Legal Obligation

Processing necessary to comply with legal and regulatory obligations, including:

- Employment law requirements
- HMRC and taxation obligations
- Pension administration
- Health and safety obligations
- Right-to-work checks
- Equality legislation requirements
- Safeguarding obligations
- DBS and safer recruitment requirements
- Regulatory reporting obligations
- Statutory investigations
- Football regulatory requirements where legally mandated

Article 6(1)(f) Legitimate Interests

Processing necessary for the legitimate interests of Birmingham City Football Club Limited and Birmingham City Women Football Club Limited, including:

- Information and cyber security monitoring
- Fraud prevention and detection
- Internal investigations
- Governance and compliance monitoring
- Business administration
- Audit and assurance activities
- Business continuity planning
- Operational resilience
- CCTV monitoring for security purposes
- Access monitoring and site security
- Incident management and security investigations
- Safeguarding support activities not arising from a specific legal obligation
- Protection of systems, facilities, assets, staff, players, supporters, visitors, contractors, and members of the public
- Stadium safety and security

Maintaining the safe, secure, and effective operation of Birmingham City Football Club Limited and Birmingham City Women Football Club Limited

Where we rely on legitimate interests, we ensure that processing is necessary, proportionate, and balanced against the rights and freedoms of individuals.

Special Category Data

Where special category data is processed, we rely on one or more of the following conditions under Article 9 UK GDPR.

Article 9(2)(a) Explicit Consent

Where explicit consent is required for specific processing activities.

Article 9(2)(b) Employment, Social Security and Social Protection

Processing necessary for employment obligations and rights, including:

- Occupational health
- Workforce management
- Sickness and absence management
- Equality monitoring
- Workplace adjustments
- Benefits administration
- Pension administration

Article 9(2)(g) Substantial Public Interest

Processing necessary for reasons of substantial public interest, including:

- Safeguarding children and individuals at risk
- Preventing or detecting unlawful acts
- Equality of opportunity and treatment
- Regulatory and governance requirements
- Protecting individuals from harm

Article 9(2)(h) Health or Social Care

Processing necessary for:

- Occupational health services
- Medical assessments
- Workplace health and safety
- Employee wellbeing support
- Health-related safeguarding matters

Criminal Offence Data

Criminal offence and DBS-related data is processed in accordance with the Data Protection Act 2018 where necessary for:

- Safer recruitment
- Safeguarding
- Legal obligations
- Regulatory requirements
- Roles involving children, vulnerable individuals, security responsibilities, financial responsibility, or positions of trust

6. Who We Share Data With

We share personal data only where necessary, lawful, proportionate, and relevant to the purpose of processing.

Internal

We may share personal data internally with:

- HR teams
- Line managers
- Department heads
- Payroll and finance teams
- IT and information security teams
- Safeguarding teams
- Medical, wellbeing, psychology, and occupational health contacts where appropriate
- Coaching, football operations, recruitment, and performance teams where relevant
- Ticketing, accreditation, stadium operations, and security teams
- Executive leadership
- Legal, governance, and compliance teams
- Access is restricted to individuals with a legitimate employment, operational, safeguarding, security, or governance need.

External

We may share personal data with:

- HMRC
- Pension providers
- Payroll providers
- Employee benefit providers
- Occupational health providers

- Training providers
- Recruitment agencies
- Reference checking providers
- DBS and vetting providers
- Legal advisers
- Insurance providers
- Auditors
- Football governing bodies and regulators where required
- Law enforcement agencies where required
- Local authorities and safeguarding bodies where required
- Medical professionals and emergency services where necessary
- Travel, accommodation, and logistics providers where required

Technology Providers (Data Processors)

Birmingham City Football Club Limited and Birmingham City Women Football Club Limited use approved technology providers to support workforce management, football operations, safeguarding, security, compliance, stadium operations, and wider business administration.

These systems may include:

- Human Resources Information Systems
- Recruitment and Applicant Tracking Systems
- Payroll and Pension Administration Systems
- Learning and Development Platforms
- Communication and Collaboration Systems
- Identity and Access Management Systems
- IT Service Management Systems
- Security Monitoring and Cybersecurity Platforms
- Document Management and Storage Systems
- Finance and Expense Management Systems
- Safeguarding and Case Management Systems
- Performance and Coaching Analysis Systems
- Ticketing, Accreditation, Access Control, and Identity Management Systems used to manage ticket allocations, matchday accreditation, hospitality access, facility access permissions, attendance records, Single Sign-On (SSO) authentication, identity verification, and security controls across systems and facilities
- CCTV, Body-Worn Video, and Security Systems

All processors operate under written data processing agreements in accordance with Article 28 UK GDPR.

7. International Transfers

Where personal data is transferred outside the UK, appropriate safeguards such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum, and/or Standard Contractual Clauses are used.

8. Data Retention

We retain personal data in accordance with our Retention Policy.

Personnel files: 7 years after employment ends

Payroll and tax records: 7 years

Pension records: up to 75 years

Recruitment records for unsuccessful candidates: 12 months

DBS records: up to 3 years where appropriate and renewed in accordance with the Clubs' safer recruitment, safeguarding, regulatory, and risk management requirements

Training records: duration of employment plus 7 years

Coaching analysis and performance records: duration of employment plus 7 years

Ticketing: 10 Years after last activity

Accreditation: 1 year

Access records: up to 2 years unless needed for investigations

Access control, security, and monitoring records: retained in accordance with security, operational, safeguarding, employment, and incident management requirements, including role-related access and audit requirements

CCTV footage: up to 30 days unless required for investigation

Health and safety records: in accordance with legal requirements

Safeguarding records: up to 75 years where safeguarding obligations apply

Personal data is securely deleted, anonymised, archived, or restricted in accordance with the Records Retention and Erasure Policy of Birmingham City Football Club Limited and Birmingham City Women Football Club Limited when it is no longer required for the purpose for which it was collected.

9. Data Security

Birmingham City Football Club Limited and Birmingham City Women Football Club Limited protect personal data using appropriate technical and organisational measures, including:

- Role-based access controls
- Encryption and secure systems
- Multi-factor authentication
- Security monitoring
- Staff training and awareness
- Regular security reviews
- Data minimisation and retention controls
- Secure transfer and storage arrangements
- Confidentiality obligations

Additional security controls, confidentiality obligations, monitoring measures, and access restrictions apply to safeguarding records, occupational health information, DBS data, disciplinary records, grievance records, investigation records, and other highly sensitive or confidential information processed by the Clubs.

10. Your Rights

You have the following rights under data protection law.

Right to Be Informed

You have the right to know how and why your personal data is used. This privacy notice explains what data we collect, how we use it, who we share it with, and how long we keep it.

Right of Access

You have the right to request a copy of the personal data we hold about you. This is commonly known as a Subject Access Request.

Right to Rectification

You have the right to ask us to correct inaccurate or incomplete personal data.

Right to Request Erasure Where Applicable

You may ask us to delete your personal data in certain circumstances. This right is not absolute, and we may need to retain data for legal, employment, safeguarding, regulatory, operational, or claims-related reasons.

Right to Restrict Processing

You may ask us to restrict how we use your personal data in certain circumstances.

Right to Object

You may object to processing where we rely on legitimate interests. We will consider your objection and whether our reasons for processing override your interests, rights, and freedoms.

Right to Data Portability

Where applicable, you may request that certain personal data is provided in a structured, commonly used, machine-readable format.

Right to Withdraw Consent

Where we rely on your consent to process personal data, you have the right to withdraw that consent at any time.

Withdrawing consent will not affect the lawfulness of any processing carried out before consent was withdrawn.

For example, you may withdraw consent for:

- Email marketing communications
- SMS marketing communications
- Direct marketing communications
- Personalised marketing activities
- Participation in surveys or promotional activities
- The use of photographs, videos, or other media content where consent is the lawful basis for processing
- Other optional activities where consent has been provided

Once consent is withdrawn, we will stop processing your personal data for the relevant purpose unless another lawful basis applies.

You can withdraw consent at any time by:

- Updating your communication preferences within your account (where available)
- Using the unsubscribe link included in marketing communications
- Contacting us at dpo@bcfc.com
- Contacting the relevant Club department managing the activity concerned

We will action requests to withdraw consent as soon as reasonably practicable and in accordance with applicable data protection laws.

Right to Challenge Automated Decision-Making and Profiling

You have rights in relation to solely automated decisions which have legal or similarly significant effects. We do not make solely automated employment decisions without appropriate safeguards.

Certain rights may be restricted where legal, employment, safeguarding, regulatory, security, law enforcement, or public safety requirements apply.

11. Data Sources

We obtain personal data from:

- Employees, workers, contractors, volunteers, and applicants
- Recruitment agencies
- Referees
- Occupational health providers
- DBS and vetting providers
- Government agencies
- HMRC
- Pension and benefits providers
- Training providers
- Line managers and colleagues
- Coaching, performance, ticketing, security, and operational systems
- CCTV, access control, and IT systems
- Safeguarding teams, authorities, or relevant third parties where applicable

12. Categories of Individuals

This notice applies to:

- Employees
- Workers
- Contractors
- Consultants
- Volunteers
- Apprentices
- Interns
- Agency workers
- Casual workers

- Former employees and workers
- Applicants where their data transfers into staff records following appointment

13. Complaints & Subject Access Requests

Complaints, data protection queries, and Subject Access Requests should be directed to:

Data Protection Officer: dpo@bcfc.com

We aim to respond within 30 days, unless an extension is permitted under data protection law.

If you are not satisfied with our response, you may contact the Information Commissioner's Office:

<https://ico.org.uk/concerns>

14,Do We Use Cookies And Other Tracking Technologies?

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

15. Updates

This privacy notice may be updated periodically to reflect changes to legal requirements, regulatory obligations, employment practices, safeguarding requirements, football operations, technology platforms, business processes, or the activities of Birmingham City Football Club Limited and Birmingham City Women Football Club Limited.

Where significant changes are made, staff will be notified through appropriate communication channels.