Walsall Football Club Data Protection Policy

Policy Owner	Version	Issue Date	Review Date
WFC Board of Directors	2	01/04/2025	01/05/2026

Policy Statement

In accordance with the General Data Protection Regulations (GDPR), the Club is committed to transparency about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations.

This Data Protection policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

Scope of the Policy

This policy applies to the HR Related Personal Data of job applicants, employees, volunteers, apprentices and former employees, but does not apply to the personal data of clients or other personal data processed for business purposes.

Definitions

"Personal data" is any information that relates to a living individual who is able to be identified from that information.

"Processing" is any use that is made of Personal Data, including collecting, storing, amending, disclosing or destroying/disposal.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data used for ID purposes.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The organisation processes HR-Related Personal Data in accordance with the following data protection principles:

1. The organisation processes personal data lawfully, fairly and in a transparent manner.
2. The organisation collects personal data only for specified, explicit and legitimate purposes.
3. The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
4. The organisation keeps accurate personal data and takes all reasonable steps to ensure that this is maintained and that inaccurate personal data is rectified or deleted without delay.
5. The organisation keeps personal data only for the period necessary for processing.
6. The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an impact assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this will be done in accordance with the organisation's absence policy or the requirements of the Disclosure and Barring Service checks.

The organisation is committed to updating HR-Related Personal Data promptly whenever an individual advises that their information has changed or is inaccurate.

Personal data gathered during employment, worker, contractor, volunteer or apprenticeship relationships will be held in the individual's personnel/contractor file (in hard copy, electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notice below.

The organisation keeps a record of its processing activities in respect of HR-Related Personal Data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Privacy notice

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to transparency about how it collects and uses that data and to meeting its data protection obligations. The organisation's privacy notice is set out below.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to any benefits such as pensions;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and eligibility to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, authorised leave, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training records, performance improvement plans and related correspondence;

- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of any trade union membership; and
- any equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The organisation collects this information in a variety of ways, such as from application forms, CVs; your passport or other identity documents eg. your driving licence; forms completed by you at the start of or during employment (such as bank details forms/training agreements); correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers/DBS checks, where appropriate and permitted by law.

Data may be stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

Why does the organisation process personal data?

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer any benefit, pension or insurance entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check all employees' entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. If regulatory requirements dictate, it will be necessary to carry out criminal records checks to ensure that individuals are permitted to undertake their role.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- operate recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain medical and/or occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;

- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the organisation relies on legitimate interests as a reason for processing your data, it has considered, via completion of an impact assessment whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Who has access to data?

Your information will be shared internally, including with members of the HR/recruitment team/payroll, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The organisation shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and, if appropriate, obtain necessary criminal records checks from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll where an external payroll provider is engaged, the provision of benefits, the provision of occupational health, and the provision of HR/legal advisory services.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, in performance of a contractual agreement, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

The organisation will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the Club's retention periods, which are typically for 6 years.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data. You are able to:

- access and obtain a copy of your data on request; (see Subject access request).
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of the above rights, please contact the HR Officer or your Line Manager. If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will inform the individual:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected directly from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to any such transfers;

- for how long their personal data is stored (or how that period is determined);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if the individual thinks the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless the individual agrees otherwise.

If the individual requests additional copies of their data, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing any additional copies.

To make a subject access request, the individual should submit their request in writing to the Club's HR Officer. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documentation it requires.

The organisation will ordinarily respond to a subject access request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to inform the individual if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation may agree to respond but will charge a fee, which will be proportionate to the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request which the organisation has already responded to. If an individual submits a request that is considered unfounded or excessive, the organisation will notify the individual that this is the case, whether or not it will be responded to and the appropriate fee.

Data security

The organisation takes the security of HR-related personal data seriously and will ensure that it has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

The organisation will only disclose personal data to third parties where there is a need to do so, e.g. to give information about your earnings to HMRC, or to seek advice from our HR or legal advisors.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

If any of the processing that the organisation carries out may result in risks to privacy, for example, CCTV monitoring. Where such processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact

assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the organisation discovers that there has been a breach of HR-Related Personal Data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their severity and/or effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

International data transfers

The organisation will not transfer HR-Related Personal Data to countries outside the EEA.

Individual responsibilities

Individuals are responsible for ensuring the organisation is able to keep their personal data up to date. Individuals should let the organisation know if any data provided to the organisation changes, for example if an individual moves house, changes their contact details, bank details or name.

Individuals may have access to the personal data of other individuals and/or our customers and clients in the course of their employment. Where this is the case, the organisation relies on those individuals to help meet its data protection obligations.

Individuals who have access to personal data must:

- only access data that they have authority to access and access it only for authorised purposes;
- not disclose data to anyone, except to individuals, whether inside or outside the organisation, who have appropriate authorisation;
- keep data secure, in particular by complying fully with security rules, including but not limited to rules on access to our premises by non authorised parties, computer access, including password protection, and secure file storage and destruction;
- not remove personal data, or electronic devices which contain, or can be used to access personal data, from the organisation's premises without prior authorisation and adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not store personal data on local drives or on any personal electronic devices, including mobile telephones, that are used for work purposes; and
- to report data breaches of which they become aware to their line manager immediately.

Failing to observe these requirements or any breach of this Data Protection Policy may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, including, but not limited to, accessing any data without authorisation, or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal without notice or pay in lieu of notice.

Training

The organisation will provide training to all individuals about their data protection and data handling responsibilities as part of the induction process and will provide any further relevant training as necessary.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Training will include ensuring that individuals are aware of their obligations in relation to keeping personal information security