# Data Protection Policy

## 1. POLICY STATEMENT

This "Data Protection Policy" has been issued by FVWL Football Limited T/A Bolton Wanderers Football Club.

Bolton Wanderers Football Club, who is registered at the University of Bolton Stadium, Burnden Way, Lostock, Bolton, BL6 6JW registered in England and Wales – 120 90433 VAT Number: 328 915576

FVWL Hotel Limited T/A Bolton Whites Hotel & Events is registered at the University of Bolton Stadium, Burnden Way, Lostock, Bolton, BL6 6JW registered in England and Wales – 120 86161 Vat Number: 328 706685.

This policy is to comply with the new "General Data Protection Regulation" ("GDPR") which came into effect on the 25th May 2018.

Under this regulation Bolton Wanderers Football Club (BWFC) and Bolton Whites Hotel & Events (BWH) are "data controllers". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this data protection policy.

As an employee for Bolton Wanderers Football Club and Bolton Whites Hotel & Events, under this regulation you will be classed as a "data user" and are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

## 2. ABOUT THIS POLICY

**2.1** The types of personal data that Bolton Wanderers Football Club may be required to include information about job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. This also applies to current, past and prospective shareholders, suppliers, customers, and others that we communicate with. The personal data, which may be held on paper or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and other regulations including (GDPR).

**2.2** This policy and any other documents referred to in it, sets out the basis on which we will process any personal data we collect, or that is provided to us by data subjects or other sources.

## 3. DEFINITION OF DATA PROTECTION TERMS

**3.1** **Data** is information which is stored electronically, or in certain circumstances paper-based filing systems.

**3.2** **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

**3.3** **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. It can also include pseudonymised data.

**3.4** **Data controllers** are the people/organisations which determine the purposes for which, and the manner in which, any personal data is processed. We are the data controller of all personal data used in our business for our own commercial purposes.

**3.5** **Data users** are employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

**3.6** **Data processors** include any person/organisation that processes personal data on our behalf and under our instructions. Employees of data controllers are excluded from this definition but it could include third party suppliers who handle personal data on behalf of Bolton Wanderers Football Club.

**3.7** **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it.

**3.8** **Sensitive personal information (SPI)** includes information about a person's gender, racial or ethnic origin, religious or similar beliefs, physical or mental health and condition, sexual orientation. It also includes genetic and biometric data (where used for ID purposes). Sensitive personal information can only be processed under strict conditions.

**3.9** **Criminal offence data** includes criminal allegations, proceedings or convictions. The disposal of this data will be in line with statutory legislation.

## 4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) processed in a fair, lawful and transparent manner

b) collected for specific, explicit, and legitimate purpose

c) adequate, relevant and non-excessive

d) kept accurate and up to date.

e) not kept for longer than is necessary for its given purpose

f) processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

g) compliant with the relevant GDPR procedures for international transfer, but;

h) not transferred to people or organisations situated in countries without adequate protection.

## 5. FAIR AND LAWFUL PROCESSING

**5.1** The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

**5.2** For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. During the course of our business as data controllers, we will ensure we process personal data in line with legislation.

## 6. PROCESSING FOR LIMITED PURPOSES

**6.1** Personal data may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

**6.2** We will only process personal data for specific purposes as permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

## 7. NOTIFYING DATA SUBJECTS

**7.1** If we collect personal data directly from data subjects, we will inform them about the following:

**(a)** The purpose or purposes for which we intend to process that personal data.

**(b)** The types of third parties (if any) which we will share or to which we will disclose that personal data.

**(c)** The means (if any) which data subjects can limit our use and disclosure of their personal data.

**7.2** If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

## 8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

**8.1** We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

## 9. ACCURATE DATA

**9.1** We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

## 10. TIMELY PROCESSING

**10.1** We will not keep personal data longer than is necessary for the purpose or purposes for which it is collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

## 11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

**11.1** We will process all personal data in line with data subjects' rights, in particular their right to:

**(a)** Request access to any data held about them by a data controller (see also **Section 15**).

**(b)** Prevent the processing of their data for direct-marketing purposes.

**(c)** Ask to have inaccurate data amended (see also **Section 9**).

**(d)** Prevent processing that is likely to cause damage or distress to themselves or anyone else.

## 12. DATA SECURITY

**12.1** We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

**12.2** We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures of security to protect the data.

**12.3** We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

**(a) Confidentiality** means that only people who are authorised to use the data have access to it.

**(b) Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

**(c) Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

**12.4** Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

**(a) Ensuring** that data is recorded on such devices only where absolutely necessary.

**(b) Using** an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.

**(c) Ensuring** that all laptops and USB drives are not left unattended and securely locked away when not in use.

**12.5 Security procedures include:**

**(a) Entry controls.** Monitored reception.

**(b) Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

**(c) Methods of disposal.** Paper documents should be confidentially shredded. Digital storage should be physically destroyed when no longer required, in line with statutory legislation.

**(d) Computer network system**. Access for data users must be via secure password log on credentials, which must never be shared and must be changed periodically in line with company policy.

**(e) Equipment.** Data users must protect the information displayed on their screens at all times and ensure they log off or screen lock their PC/laptop when it is unattended.

## 13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

**13.1** We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

**(a)** The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

**(b)** The data subject has given their consent.

**(c)** The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

**(d)** The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

**(e)** The transfer is authorised by the relevant data protection authority at the point we have confirmation of adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

## 14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

**14.1** We may share personal data we hold with any of our group companies; as defined in section 1159 of the UK Companies Act 2006 and as detailed at the start of this policy.

**14.2** We may also disclose personal data we hold to third parties as defined below:

**(a)** In the event that we sell or buy any business or assets, we may disclose your personal data we hold, to the prospective seller or buyer as it will be regarded as a business asset.

## 15. DEALING WITH SUBJECT ACCESS REQUESTS

**15.1** Data subjects must make a formal request for information that we hold about them.

**15.2** What forms of ID will I need to provide in order to access this?

BWFC accepts the following forms of ID when information on your personal data is requested:

- Passport
- Driving licence
- Birth certificate
- Utility bill (dated within the last 3 months)

Upon seeing any form of ID, a representative from the Club will sign to say they have seen it, on what date and that any photo ID is a true likeness of the person requesting their data.

**15.3** Employees should not feel pressurised into disclosing personal information at any time and should notify their line manager if they are worried about a request.

**15.4** All subject access requests must be forwarded to the DP Office dpo@bwfc.co.uk immediately.

## 16. CHANGES TO THIS POLICY

**16.1** We reserve the right to change this policy at any time and will be reviewed annually.

**16.2** Any substantial changes will be notified through the appropriate channels.

**All employees who deal with personal data need to ensure they understand the principles of protecting individuals data at all times and to ensure they read all policies and procedures to prevent breaches.**

**Failure to follow the Company's rules on data security will be dealt with via the Company's disciplinary procedure.**

Effective Date: **25th May 2018**

Review Date: **July 2020**

Updated: **October 2020**

**If you have any questions about this Data Protection Policy, please contact the Data Protection Office on dpo@bwfc.co.uk**

I, …… acknowledge that on

…… (date), I received a copy of the Bolton Wanderers Football Club, Data Protection Policy, and that **I have read and understood it**.

**Signature** ……

**Name** ……

**Date** _ _ / _ _ / _ _ _ _