The Albion Foundation General Data Protection Regulation Policy

CONTENTS:

1. INTRODUCTION

The Albion Foundation *(hereinafter referred to as **"TAF")*** recognises and understands that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation. TAF also recognises that the lawful and correct treatment of information is very important to our successful operation and in maintaining confidence between us and those with whom we carry out business.

TAF adheres to and fully endorses the principles of the General Data Protection Regulations (GDPR 2018).

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and have been developed to meet the best practices of business records management, with the direct aim of ensuring a robust and structured approach to document control and systems.

This policy relates to all relevant individuals with whom TAF processes data either in manual or electronic records. These relevant individuals are defined as – but not restricted to - job applicants, employees, volunteers, self-employed contractors and participants (and/or responsible adults). These are referred to in this policy as relevant adults.

This policy will be reviewed every 2 years as a minimum and/or in the event of any change in circumstances relating to this policy. See version control.

2. DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information (e.g. name, address, telephone number, etc.).

"Special categories of personal data" is information, which relates to an individual's health, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership.

"Criminal offence data" is data, which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. DATA PROTECTION PRINCIPLES

Under Article 6 of GDPR, all personal data obtained and held by TAF must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a. Data processing will be fair, lawful and transparent.
b. Data will be collected for specific, explicit, and legitimate purposes only.
c. Data collected will be adequate, relevant and limited to what is necessary for the purposes of processing. See appendix 2 for retention periods.
d. Data will be kept accurate and up to date. Data that is found to be inaccurate will be rectified or erased without delay.
e. Data is not kept for longer than is necessary for its given purpose (see retention schedule).
f. Data will be 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. We will comply with the relevant GDPR procedures for international transferring of personal data.

4. TYPES OF DATA HELD

TAF stores and/or shares several categories of personal data in order to carry out effective and efficient processes. TAF stores employee/volunteer data in a personnel file and within our computer systems, for example, HR software. TAF also stores information on participants (within our CRM/booking software) and shares this with funding agencies (but this is only for the purposes of meeting specific funding criteria).

Specifically, we hold the following types of data:

EMPLOYEES/VOLUNTEERS

a. Personal details such as name, address, phone numbers, etc.
b. Information gathered via the recruitment process.
c. Details relating to pay administration such as National Insurance numbers, bank account details and tax codes.
d. Medical or health information.
e. Information relating to your employment with us (e.g. performance records, disciplinary information, etc.)

PARTICIPANTS

a. Personal details such as name, address, phone numbers, etc.
b. Sensitive information such as medical history, ethnicity, etc.

All of the above information is required for our processing activities. More information on those processing activities is included in our privacy notice.

5. EMPLOYEE RIGHTS

Employees have the following rights in relation to the personal data we hold on you:

a. The right to be informed about the data we hold on you and what we do with it.
b. The right of access to the data we hold on you. More information on this can be found in the section headed “Access to Data” below and in our separate policy on Subject Access Requests”;
c. The right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as ‘rectification’.
d. The right to have data deleted in certain circumstances. This is also known as ‘erasure’.
e. The right to restrict the processing of the data.
f. The right to transfer the data we hold on you to another party. This is also known as ‘portability’.
g. The right to object to the inclusion of any information.
h. The right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

6. RESPONSIBILITIES.

In order to protect the personal data of relevant individuals, those within TAF who must process data as part of their role have been made aware of our policies on data protection.

TAF have also appointed employees with responsibility for reviewing and updating our data protection policies and processes (Director of TAF).

7. LAWFUL BASES OF PROCESSING.

TAF acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, TAF may seek to rely on the individuals consent in order to process data.

However, TAF recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, TAF will do so on a specific and individual basis where appropriate. Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

8. ACCESS TO DATA

As stated above, individuals have a right to access the personal data that TAF store on them. To exercise this right, individuals should make a 'Subject Access Request'. TAF will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

9. DATA DISCLOSURES

TAF may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a. Any employee benefits operated by third parties.
b. Disabled individuals - whether any reasonable adjustments are required to assist them at work.
c. Individuals' health data - to comply with health and safety or occupational health obligations towards an individual.
d. For Statutory Sick Pay purposes.
e. HR management and administration - to consider how an individual's health affects his or her ability to do their job.
f. The smooth operation of any employee insurance policies or pension plans;
g. To assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.
h. To share individual's data with funding agencies.

These kinds of disclosures will only be made when strictly necessary for the purpose.

10. DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc. when unattended. No files or written information of a confidential nature are to be left where unauthorised people can read them.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

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.
c. Ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the TAF policy on data security may be dealt with via the TAF's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

11. THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the TAF's commitment to protecting data.

12. INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

13. REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, TAF will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, TAF will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

14. TRAINING

New TAF employees must read and understand the policies on data protection as part of their induction.

All TAF employees must complete an e-training course covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller (Head of Operations) for TAF is trained appropriately in their role under the GDPR.

All TAF employees who need to use relevant computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the TAF's policies and procedures.

15. GDPR Compliance

The designated data protection lead is:

Shin Aujla, Head of Operations (Shin.aujla@albionfoundation.co.uk)

The Albion Foundation has access to professional advice from:

- The Data Protection Lead at WBA FC
- Local Authority
- External Partners

16. Appendix 1.

THE ALBION FOUNDATION (TAF) - GUIDELINES FOR DATA PROTECTION

1. All staff have a duty to make sure that they comply with the data protection principles, which are set out in this (and the club's) Data Protection Policy. In particular, Staff must ensure that all participant records are:

    - Accurate;
    - Up-to-date.
    - Fair.
    - Kept and disposed of safely.

2. Staff must seek advice from The Head of Operations, to hold or process data that is:

    - Non-standard data.
    - Sensitive data.

    Sensitive or non-standard data may be disclosed to a third party, if The Head of Operations is not available. This should only happen in very limited circumstances (e.g. a participant is injured and unconscious, but in need of medical attention, and staff tell the hospital that the player is on medication).

3. All Staff will be responsible for ensuring that all data is kept securely.

4. Staff must not disclose personal data to any participant, unless for normal technical or pastoral purposes, without prior agreement from the Head of Operations.

5. Staff shall not disclose personal data to any other staff member except with the prior agreement of The Head of Operations.

6. Before processing any personal data, all staff should consider the checklist.

    Staff Checklist for Recording Data:

    - Do you really need to record the information?
    - Is the information 'personal' or 'sensitive'?
    - If it is sensitive, do you have the data subject's express consent?
    - Has the participant been told that this type of data will be processed?
    - Are you authorised to collect/store/process the data?
    - If yes? Have you checked with the data subject that the data is accurate?
    - Are you sure that the data is secure?

17. Appendix 2.

GENERAL INDUSTRY GUIDELINES FOR RETENTION OF INFORMATION

Types of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms / interview notes	At least 1 year from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR 1994
Participants' records, including technical/academic achievements, and conduct	3 academic years from the date the participant leaves - in case of litigation for negligence.	Limitation period for negligence