

Data Retention Policy

1. Introduction

This Policy sets out the obligations of Kidderminster Harriers Football Club Limited, a company registered in England under number :484523, whose head office is at Aggborough Stadium, Hoo Road, Kidderminster, Worcestershire, DY10 1NB, England, United Kingdom (“the Company”) (“the Company”) regarding data protection and the rights of employees and clients/customers (“data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation; or
- f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company for the purpose of providing relevant promotional messages and/or to act as a general point of contact for specific and relevant communications only and/or maintain relevant working relationships, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

2. Aims and Objectives

- 2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.
- 2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

- 3.1 This Policy applies to all personal data held by the Company.
- 3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:
 - a) Secure offices as the Company's premises at Aggborough Stadium in Kidderminster, Worcestershire.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Privacy Policy.

- 4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
- 4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

- 5.1 The following technical measures are in place within the Company to protect the security of personal data:
 - a) Personal data may only be transmitted over secure networks;
 - b) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
 - c) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
 - d) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
 - e) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient;

- f) All personal data transferred physically should be transferred in a suitable container marked “confidential”;
- g) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the data processor.
- h) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
- j) Personal data must be handled with care at all times and should not be left unattended or on view;
- k) Computers used to view personal data must always be locked before being left unattended;
- l) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise;
- m) All personal data stored electronically should be backed up. All backups should be encrypted;
- n) All electronic copies of personal data should be stored securely using passwords and encryption;
- o) All passwords used to protect personal data should be changed regularly and should must be secure;
- p) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- q) All software should be kept up-to-date. Security-related updates should be installed;
- r) No software may be installed on any Company-owned computer or device without approval; and
- s) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the data processor to ensure that the appropriate consent is obtained and that no data subjects have opted out.

5.2 The following organisational measures are in place within the Company to protect the security of personal data:

- a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company’s responsibilities under the GDPR and under the Company’s Privacy Policy;
- b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
- c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

- e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Privacy Policy;
- i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Privacy Policy;
- j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Privacy Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- 6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted;
- 6.2 Personal data stored in hardcopy form shall be shredded;

7. Data Retention

- 7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
- 7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
- 7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:
 - a) The objectives and requirements of the Company;
 - b) The type of personal data in question;
 - c) The purpose(s) for which the data in question is collected, held, and processed;
 - d) The Company's legal basis for collecting, holding, and processing that data;
 - e) The category or categories of data subject to whom the data relates
- 7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can

be regularly reviewed against those criteria.

- 7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria
001	Employee Personal Data	Contact Details, Salary details both current and past, DBS information, NI number, passports, driving licences, sick notes, HRMC information, letters, emails, other relevant details provided relevant for the employee to work at the Company. Provided for use to employ the employee	7 years from date of employee leaving the Company	7 years from date of employee leaving the Company
002	Client and Customer Personal Data	Client and customer personal contact details Details of company information including email addresses, phone numbers, bank details, addresses. Data of invoices and payment receipts provided at the point of purchase of club products (including but not limited to Season Tickets, match tickets, match hospitality, commercial hospitality and commercial sponsorship) for use to provide relevant promotional messages and/or to act as a general point of contact for specific and relevant communications only.	5 years from the Client and/or supporter no longer being an active client or supporter	Indefinite
003	Supplier/Contractor Personal Data	Supplier/Contractor personal contact details Details of company information including email addresses, phone numbers, bank details, addresses Data of invoices and payment receipts Provided for use to assist us to maintain relevant working relationships.	24 Months	Indefinite

8. Roles and Responsibilities

- 8.1 The Company's Data Protection Officer is Keith Mansell.
- 8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Privacy Policy), and with the GDPR and other applicable data protection legislation.
- 8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods.
- 8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.